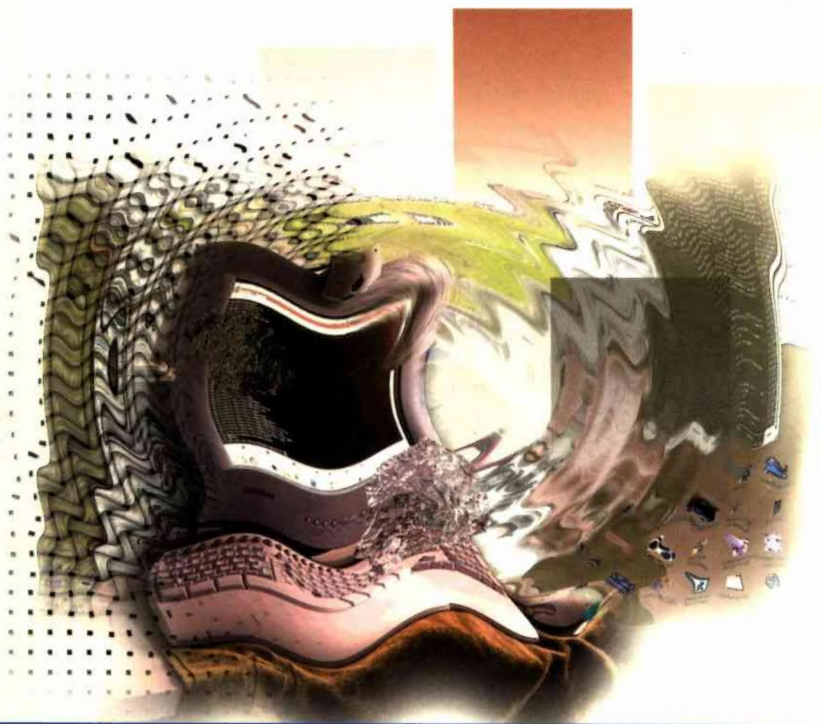


رایانه کار درجه ۲

استاندارد بین المللی ۴۲/۲۸-۳
مطابق با استاندارد جدید

ویروس های کامپیوتری





رایانه کار درجه دو

مهارت هشتم

ویروس‌های کامپیوتری



مولفین

مهندس مجید سبزه‌علی گل

مهندس سید علی موسوی

مهندس مهدی قربانی

موسوی، علی
رایانه کار درجه دو: مهارت هشتم ویروس‌های کامپیوتری / مؤلفین
علی موسوی، مجید سبزی علی گل، مهدی قربانی. - تهران: صفار:
اشراقی، ۱۳۸۳.
۸۰ ص.: مصور.

ISBN 964-388-070-2

فهرست‌نویسی بر اساس اطلاعات فیپا.
عنوان دیگر: رایانه کار درجه ۲: ویروس‌های کامپیوتری (مهارت
هشتم).

۱. ویروس‌های کامپیوتر -- دسته‌نامه‌ها. الف. سبزی علی گل، مجید،
۱۳۵۲ - ب. قربانی، مهدی، ۱۳۴۹ - ج. عنوان. د. عنوان: رایانه
کار درجه ۲: ویروس‌های کامپیوتری (مهارت هشتم).
۸۵ م ۷۶/۷۶/۷۶ QAV ۵/۸۴

۸۳-۲۶۵۴۷

کتابخانه ملی ایران

فهرست‌نویسی پیش از انتشار: انتشارات صفار

شناسنامه کتاب

نام کتاب : رایانه کار درجه ۲ ویروس‌های کامپیوتری (مهارت هشتم)
تألیف : سید علی موسوی - مجید سبزی علی گل - مهدی قربانی
طرح جلد : فرهاد کمالی
لیتوگرافی : پویش
چاپ متن : چاپخانه گنج شایگان
چاپ جلد : چاپخانه ظفر
نوبت چاپ : اول - ۱۳۸۳
شمارگان : ۳۳۰۰ نسخه
ناشر : انتشارات صفار - اشراقی
قیمت : ۹۰۰۰ ریال
مرکز پخش : پخش کتاب بینش (۵) ۶۴۰۸۴۸۷

حق چاپ محفوظ و مخصوص ناشر می‌باشد ۱۳۸۳

www.nasherin.com/saffar

saffar@nasherin.com

شابک ۹۶۴-۳۸۸-۰۷۰-۲

ISBN 964-388-070-2

تمامی حقوق مادی و معنوی این اثر متعلق به ناشر است. تکثیر تمام یا قسمتی از این اثر بصورت حروفچینی یا چاپ
مجدد، چاپ افست، پلی‌کپی و انواع دیگر چاپ ممنوع است. متخلفان تحت پیگرد قانونی قرار خواهند گرفت.

تعریف :

رایانه کار درجه دو : کسی است که از عهده توانایی شناخت مبانی و مفاهیم کامپیوتر ، کار با سیستم عامل Windows XP ، کار با Word ، کار با Excel ، کار با Access ، کار با PowerPoint و کار با اینترنت برآید.

رایانه کار درجه ۲		
کد شناسایی	۱۱۰۱۰۳۳۰۱-۷	
شماره درس	۸۹۹۴ - ۸۹۹۵	
کد استاندارد بین المللی	۳-۴۲/۳۸	
سال تدوین استاندارد	۱۳۸۲	
تعداد واحد	نظری	۵،۵
	عملی	۶،۵
	کل	۱۲
مدت دوره	نظری	۱۶۰ ساعت
	عملی	۲۹۰ ساعت
	کل	۴۵۰ ساعت
نمره قبولی (از ۲۰)	نظری	۱۰
	عملی	۱۴

مهارت اول	مبانی کامپیوتر
مهارت دوم	سیستم عامل Dos
مهارت سوم	ویندوز XP (۱)
مهارت چهارم	MS Word XP
مهارت پنجم	MS Excel XP
مهارت ششم	MS Access XP
مهارت هفتم	MS PowerPoint XP
مهارت هشتم	ویروس های کامپیوتری
مهارت نهم	اینترنت
مهارت دهم	Outlook Express 6

رایانه کار درجه دو

فهرست مطالب

مقدمه ۶

توانایی اول : آشنایی با برنامه‌های مخرب ۸

- ۱-۱ آشنایی با برنامه‌های مخرب ۹
- ۱-۲ انواع برنامه‌های مخرب ۹
- ۱-۳ آشنایی با راههای انتقال برنامه‌های مخرب ۱۰
- ۱-۴ آشنایی با مفهوم ویروس کامپیوتری ۱۰

توانایی دوم : آشنایی با انواع ویروس ۱۵

- ۲-۱ انواع ویروس از نظر محل تاثیر گذاری ۱۶
 - ۲-۱-۱ ویروسهای تاثیرگذار بر روی فایل‌های اجرایی ۱۶
 - ۲-۱-۲ ویروسهای تاثیرگذار بر روی فایل‌های غیر اجرایی ۱۶
 - ۲-۱-۳ ویروسهای تاثیرگذار بر روی رکورد راهانداز (Boot Record) ۱۷
 - ۲-۱-۴ ویروسهای تاثیرگذار بر روی جدول Partition ۱۷
- ۲-۲ روشهای انتقال ویروس ۱۷
 - ۲-۲-۱ انتقال ویروس از طریق دیسکت یا سی‌دی آلوده ۱۷
 - ۲-۲-۲ انتقال ویروس از طریق شبکه ۱۸
 - ۲-۲-۳ انتقال ویروس از طریق اینترنت ۱۸

توانایی سوم : تشخیص ویروسی شدن سیستم ۲۲

- ۳-۱ اصول تشخیص ویروسی شدن سیستم ۲۳
 - ۳-۱-۱ کند شدن سیستم ۲۳
 - ۳-۱-۲ اشکال در راهاندازی سیستم ۲۳
 - ۳-۱-۳ اشکال در اجرای فایل‌های اجرایی ۲۴
 - ۳-۱-۴ کند شدن ارتباط با اینترنت ۲۴

توانایی چهارم : مقابله با ویروسی شدن سیستم ۲۸

- ۴-۱ روشهای مقابله با ویروسها ۲۹

- ۴-۲ روشهای مقابله با ویروسهای اینترنتی..... ۳۰
- ۴-۳ آشنایی با مراحل پاکسازی سیستم آلوده..... ۳۱
- ۴-۳-۱ پاکسازی ویروسهای مقیم در حافظه..... ۳۲
- ۴-۳-۲ پاکسازی ویروسهای غیر مقیم در حافظه..... ۳۲
- ۴-۳-۳ پاکسازی ویروسیهای اینترنتی..... ۳۲
- ۴-۴ آشنایی با نرم افزارهای ضد ویروس..... ۳۳
- ۴-۵ روشهای مقابله نرم افزارهای ضد ویروس با ویروسها..... ۳۳

توانایی پنجم : کار با نرم افزار ضد ویروس McAfee..... ۴۰

- ۵-۱ آشنایی با نرم افزار McAfee..... ۴۱
- ۵-۲ نصب نرم افزار McAfee..... ۴۱
- ۵-۳ آشنایی با محیط کار نرم افزار McAfee..... ۴۴
- ۵-۳-۱ مرکز امنیت من..... ۴۵
- ۵-۳-۲ سربرگ ویروس یابی..... ۴۶
- ۵-۳-۳ سربرگ دیوار آتش شخصی..... ۴۷
- ۵-۳-۴ سربرگ سرویس اختفاء..... ۴۹
- ۵-۳-۵ سربرگ نابودکننده هرز نامه..... ۵۰
- ۵-۴ ویروس یابی با نرم افزار McAfee..... ۵۱
- ۵-۵ بروزرسانی نرم افزار McAfee..... ۵۳

توانایی ششم : کار با نرم افزار ضد ویروس Norton..... ۶۰

- ۶-۱ آشنایی با نرم افزار Norton Antivirus..... ۶۱
- ۶-۲ نصب نرم افزار Norton Antivirus..... ۶۱
- ۶-۳ شناسایی و پاکسازی ویروسها با نرم افزار Norton Antivirus..... ۶۷
- ۶-۴ بروزرسانی نرم افزار Norton Antivirus..... ۷۱

مقدمه

پیشرفت سریع تکنولوژی، بویژه فنآوری اطلاعات و ارتباطات (ICT)، روز به روز چشم اندازه‌ها و افق‌های روشن‌تری را جهت تسخیر قُلل علمی، فنی و صنعتی و حل مشکلات و مسائل بشر ارائه می‌کند و تک‌تک افراد جامعه را به تلاش مضاعف در کسب مهارت‌های رایانه‌ای و کاربرد آنها در سایر علوم مُلزم می‌سازد، بنحوی که امروزه افراد و جوامع ناتوان در بکارگیری فن‌آوریهای جدید رایانه‌ای را بی‌سواد تلقی می‌کنند، گواه این امر پذیرش و اجرای دوره‌های مهارت رایانه‌کار و سایر مهارت‌های مرتبط فنآوری اطلاعات از سوی وزارت آموزش و پرورش است.

خوشبختانه سازمان آموزش فنی و حرفه‌ای کشور نیز که متولی آموزش‌های فنی و حرفه‌ای و تدوین استانداردهای مربوطه در کشور است همه ساله و همگام با پیشرفت فن‌آوری و نیاز جامعه، استانداردهای لازم را بازنگری و اصلاح می‌نماید به همین منظور نگارش دوم استانداردهای رایانه‌کار با رویکرد توانایی بکارگیری **Windows XP** و **Office XP** اصلاح گردیده است.

استاندارد آموزشی رایانه‌کار درجه دو در قالب مهارت‌های زیر ارائه شده است :

رایانه‌کار درجه دو				
مهارت	عنوان مهارت	زمان آموزش (ساعت)		
		نظری	عملی	کل
اول	مبانی کامپیوتر	۸/۵	۱۲	۲۰/۵
دوم	سیستم عامل Dos	۷	۱۰	۱۷
سوم	ویندوز XP (۱)	۴۰/۵	۷۳/۵	۱۱۴
چهارم	MS Word XP	۲۱	۴۸	۶۹
پنجم	MS Excel XP	۲۱	۳۷	۵۸
ششم	MS Access XP	۲۲	۵۳	۷۵
هفتم	MS PowerPoint XP	۲۰	۳۲	۵۲
هشتم	ویروس‌های کامپیوتری	۶	۱۲	۱۸
نهم	اینترنت	۷	۵	۱۲
دهم	Outlook Express 6	۷	۷/۵	۱۴/۵
جمع کل (ساعت)		۱۶۰	۲۹۰	۴۵۰

در راستای تدوین کتب آموزشی خودآموز ، مولفین **گروه آموزش مهارت (گام)** بر اساس سالها تجربه تدریس ، تحقیق و برنامه‌ریزی در علوم مختلف رایانه‌ای و با عنایت به نیاز مبرم کارآموزان ، دانش آموزان و سایر علاقه‌مندان به فراگیری آموزش‌های فنی و حرفه‌ای ، اقدام به تهیه و تدوین این مجموعه بر اساس جدیدترین سرفصل **استانداردهای مهارت فنی و حرفه‌ای و مطابق با آخرین تغییرات کتاب‌های درسی کار دانش** با ویژگی‌های منحصر به فرد زیر نموده‌اند :

- شیوه آموزشی این سری از کتابها خودآموز و گام به گام می باشد ، به همین منظور و جهت رعایت پیوستگی مطالب و سهولت در یادگیری ، در مواردی سرفصل‌های استاندارد جابجا شده است .
- تعاریف اصطلاحات و مفاهیم کلیدی به صورت پر رنگ و با رنگ متمایز مشخص شده‌اند.
- چکیده‌ای از رؤس مطالب و موضوعات ارائه شده در هر فصل ، در ابتدای همان فصل آورده شده است همچنین قبل از تشریح اغلب موضوعات ، جهت فراگیری آسان نوآموزان ، دسته بندی مناسبی از تیتیر مطالب آن موضوع ارائه شده است .
- هر گام عملی با علامت ☒ در ابتدای آن مشخص شده است و حتی‌المقدور تصاویر لازم برای هر گام آورده شده است.
- بر روی تصاویر عملکرد گزینه‌ها و دکمه‌ها به همراه سایر توضیحات لازم مشخص شده است.
- نکات اساسی و تکمیلی در کادرهای مخصوص نکته ، آورده شده است.
- دکمه‌ها ، نمادها و آیکن‌های لازم برای تشریح هر موضوع ، در جای خود و در داخل متن آورده شده است ، ضمن اینکه عملکرد آنها به صورت جداگانه در جدول‌ها ویژه یا بر روی تصویر مشخص شده است.
- در انتهای هر فصل مجموعه‌ای از سئوالات تشریحی ، تستی و دستور کار آزمایشگاه برای تکمیل مهارت دانش‌آموزان و آشنایی آنها با نمونه سئوالات امتحانی آورده شده است.

در پایان از کلیه دست‌اندرکاران مجموعه ، بویژه **آقای اشراقی** مدیریت محترم انتشارات **صفار** تشکر می‌کنیم و پیشاپیش نظرات **منتقدان** و **یاربگران** را در جهت ارتقاء سطح کمی و کیفی مجموعه گرامی می‌داریم.



گروه آموزش مهارت

Gaam@Email.com

توانایی اول

آشنایی با برنامه‌های مخرب

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می‌رود که :

- ☒ برنامه‌های مخرب را تعریف نماید.
- ☒ انواع برنامه‌های مخرب را نام ببرد.
- ☒ راههای انتقال برنامه‌های مخرب را بداند.
- ☒ ویروس کامپیوتری را تعریف نماید.
- ☒ خواص ویروسهای کامپیوتری را نام ببرد.

زمان نظری : ۲ ساعت

زمان عملی : -----



۱-۱ آشنایی با برنامه‌های مخرب

هر نرم‌افزار با توجه به دستورالعمل‌هایی که در آن وجود دارد، عملیات خاصی را انجام می‌دهد. برنامه‌نویس یک نرم‌افزار با توجه به هدفی که از ایجاد نرم‌افزار دارد، یکسری دستورالعمل‌هایی را در نرم‌افزار پیشبینی می‌کند. حال اگر یک برنامه‌نویس قصد داشته باشد برنامه‌ای تولید کند که به برنامه‌های دیگر و فایلها و اطلاعات کامپیوتر آسیب برساند، یکسری دستورالعمل را جهت نابود کردن و یا خراب کردن فایل‌های کامپیوتر در نرم‌افزار قرار می‌دهد.

برنامه‌های مخرب با اهداف مختلفی تولید می‌شوند. گاهی اوقات یک برنامه مخرب جهت ضربه زدن به شرکت‌های رقیب نرم‌افزاری و بدنام کردن محصولات شرکت رقیب تهیه می‌شود. گاهی اوقات برنامه مخرب توسط برنامه‌نویسان حرفه‌ای جهت ضربه زدن به اطلاعات شبکه‌های کامپیوتری کشورهای دیگر و یا نشان دادن قدرت نرم‌افزاری خود و مطرح کردن نام یک گروه در دنیای برنامه‌نویسان می‌باشد.

برنامه مخرب

برنامه‌هایی هستند که با هدف آسیب رساندن به نرم‌افزارهای دیگر و یا نابود کردن اطلاعات کامپیوتر تهیه می‌شوند.

۱-۲ انواع برنامه‌های مخرب

برنامه‌های مخرب از لحاظ نوع آسیب رسانی می‌توان به سه دسته زیر تقسیم کرد :

- **برنامه‌های مخرب نرم‌افزارها**
این برنامه‌ها برای ضربه زدن و نابود کردن یک نرم‌افزار مشخص یا محصولات یک شرکت خاص تولید می‌شوند.
- **برنامه‌های مخرب سخت‌افزارها**
این برنامه‌ها جهت آسیب رساندن به یک قطعه سخت‌افزاری نظیر مانیتور ، کارت گرافیک ، دیسک سخت ، آی‌سی BIOS و تهیه می‌شوند.
- **برنامه‌های مخرب اطلاعات**
این برنامه‌ها فقط به اطلاعات موجود در بانکهای اطلاعاتی آسیب می‌رساند.



- برنامه‌های جاسوسی و نفوذ کننده

این برنامه‌ها توسط نفوذگرها (Hackers) جهت نفوذ به شبکه‌های کامپیوتری ، کامپیوترهای شبکه ، کامپیوترهای شخصی و ... تهیه می‌شوند.

۳-۱ آشنایی با راههای انتقال برنامه‌های مخرب

برنامه‌های مخرب را همانند دیگر برنامه‌های کامپیوتری از طرق مختلفی می‌توان بر روی کامپیوترها منتقل کرد. ولی اگر دریافت کننده این برنامه بداند که ممکن است این برنامه مخرب باشد آن را اجرا نمی‌کند. به همین منظور تهیه کنندگان برنامه‌های مخرب ، سعی می‌کنند این برنامه‌ها را بدون اطلاع کاربران روی کامپیوتر آنها منتقل کرده و اجرا کنند و یا اینکه به روشهای مختلفی اطمینان کاربران کامپیوتر را جلب کنند و برنامه‌های مخرب را برنامه‌ای مفید و سودمند جلوه دهند.

۴-۱ آشنایی با مفهوم ویروس کامپیوتری

ویروس کامپیوتری به برنامه‌های مخرب کوچکی گفته می‌شود که مخفیانه وارد کامپیوتر می‌شوند و بدون اطلاع و اختیار کاربر خود را تکثیر می‌کنند. پس هر برنامه مخرب ، ویروس نیست. در واقع ویروس کامپیوتری نوعی برنامه مخرب است که خواص زیر را داشته باشد :

- بسیار کوچک و کم حجم باشد
- بدون اطلاع کاربر بر روی کامپیوتر او منتقل شود
- بدون اطلاع کاربر تکثیر شده و به کامپیوترهای دیگر منتقل شود

ویروس کامپیوتری

ویروس کامپیوتری به برنامه‌های مخرب کوچکی گفته می‌شود که مخفیانه وارد کامپیوتر می‌شوند و بدون اطلاع کاربر خود را تکثیر می‌کنند.

نام ویروس به این علت روی اینگونه از برنامه‌ها گذاشته شده است که عملکردی مشابه ویروس‌های بیولوژیک دارند. یک ویروس بیولوژیک از طرق مختلفی ممکن است وارد بدن انسان شود و ممکن است تا مدت زیادی به فعالیت مخفیانه در بدن بپردازد و پس از مدتی علائم وجود ویروس مشخص شود. یک ویروس کامپیوتری نیز از طرق مختلفی ممکن است وارد کامپیوتر شود و تا مدتها به فعالیت خود



ادامه دهد و پس از مدتی اختلالاتی را در کامپیوتر ایجاد نماید. ویروس‌های کامپیوتری می‌توانند به اطلاعات و برنامه‌های موجود در کامپیوتر آسیب رسانده و آنها را از بین ببرند.

ویروس‌های کامپیوتری توسط برنامه‌نویسان مجرب جهت آسیب رساندن به شرکت‌های رقیب نرم‌افزاری، مختل کردن شبکه‌های کامپیوتری یا سایر مقاصد مشابه نوشته می‌شوند و همراه برنامه‌های قفل شکسته، برنامه‌های رایگان، از طریق اینترنت و غیره به کامپیوترهای دیگر انتقال می‌یابند.



- ۱ - برنامه‌های مخرب را تعریف نمایید.
- ۲ - انواع برنامه‌های مخرب را نام ببرید.
- ۳ - ویروس کامپیوتری را تعریف نمایید.
- ۴ - خواص ویروسهای کامپیوتری را نام ببرید.



۱- انواع برنامه‌های مخرب کدامند؟

- الف) برنامه‌های مخرب نرم‌افزارها و سخت‌افزارها
- ب) برنامه‌های مخرب اطلاعات و برنامه‌های جاسوسی و نفوذکننده‌ها
- ج) برنامه‌های مخرب سخت‌افزارها
- د) الف و ب

۲- کدامیک خواص ویروس کامپیوتری نیست؟

- الف) بسیار کوچک و کم حجم است.
- ب) بدون اطلاع کاربر بر روی کامپیوتر او منتقل می‌شود.
- ج) بدون اطلاع کاربر با قراردادن دو دیسک در کنار یکدیگر، از یک دیسک به دیسک دیگر منتقل می‌شود.
- د) بدون اطلاع کاربر تکثیر شده و به کامپیوترهای دیگر منتقل می‌شود

۳- هدف از نوشتن ویروسهای کامپیوتری است.

- الف) آسیب رساندن به شرکت‌های رقیب نرم‌افزاری
- ب) مختل کردن شبکه‌های کامپیوتری
- ج) آسیب رساندن به اینترنت
- د) الف و ب



فصل	سؤال	الف	ب	ج	د
اول	۱				✓
	۲			✓	
	۳				✓

توانایی دوم

آشنایی با انواع ویروس

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ✓ انواع ویروس از نظر محل تاثیر گذاری را نام ببرد.
- ✓ عملکرد ویروس های تاثیر گذار بر روی فایل های اجرایی را شرح دهد.
- ✓ عملکرد ویروس های تاثیر گذار بر روی فایل های غیر اجرایی را شرح دهد.
- ✓ عملکرد ویروس های تاثیر گذار بر رکورد راه انداز را شرح دهد.
- ✓ عملکرد ویروس های تاثیر گذار بر جدول Partition را شرح دهد.
- ✓ روش های انتقال ویروس به کامپیوتر را نام ببرد.

زمان نظری : ۱ ساعت

زمان عملی : _____



۲-۱ انواع ویروس از نظر محل تاثیر گذاری

ویروس‌ها مثل سایر برنامه‌های کامپیوتری نیاز به محلی برای ذخیره خود دارند، با این تفاوت که ویروس‌ها محلی را انتخاب می‌کنند که برای رسیدن به اهداف شوم خود نزدیکتر و در دسترس تر باشند. محل‌هایی که برای جایگیری ویروس‌ها محبوبیت بیشتری دارند بشرح زیر می‌باشند:

- فایل‌های اجرایی
- فایل‌های غیر اجرایی
- رکورد راه انداز (Boot Record)
- جدول پارتیشن (Partition Table یا Master Boot Record)

در ادامه با انواع ویروس‌ها از نظر محل تاثیر گذاری بیشتر آشنا خواهیم شد:

۲-۱-۱ ویروس‌های تاثیرگذار بر روی فایل‌های اجرایی

اکثر ویروس‌ها بطور انگل وار به فایل‌های اجرایی می‌چسبند و آنها را آلوده می‌کنند تا پس از اجرا شدن آنها فعال شده و ضمن تکثیر خود، اطلاعات را از بین ببرند. به همین منظور اغلب نرم افزارهای ضد ویروس، فایل‌های اجرایی یا انشعاب‌های زیر را بررسی یا پاکسازی می‌کنند:

.EXE ، .COM ، .SYS ، .BIN ، .OVL ، .DLL ، .SCR

بنابراین فایل‌های اجرایی با انشعاب‌های فوق از اصلی‌ترین محل‌های جایگیری ویروس‌ها می‌باشند.

۲-۱-۲ ویروس‌های تاثیرگذار بر روی فایل‌های غیر اجرایی

بندرت ویروس‌ها در فایل‌های غیر اجرایی مثل فایل‌های متنی یا بانک‌های اطلاعاتی جای می‌گیرند. از ویروس‌های تاثیرگذار بر روی فایل‌های غیر اجرایی می‌توان به ویروس‌هایی اشاره کرد که در انتهای اسناد Word یا Excel خود را پنهان می‌کنند. این ویروس‌ها بصورت دستورات نرم‌افزارهای Word یا Excel هستند که پس از باز شدن سند به صورت خودکار اجرا می‌شوند. معمولاً آثار مخرب ویروس‌ها بر روی فایل‌های غیر اجرایی نمایان می‌شود و کمتر مشاهده شده است که ویروس‌ها، خود را در فایل‌های غیر اجرایی پنهان کنند.



۳-۱-۲ ویروسهای تاثیرگذار بر روی رکورد راهانداز (Boot Record)

برخی دیگر از ویروس ها علاقه خاصی به پنهان شدن در رکورد راهانداز دارند زیرا رکورد راه انداز، واحد راهاندازی DOS است که در سکتور شماره صفر دیسک سخت یا فلاپی دیسک قرار دارد و اینگونه از ویروسها با قرار گرفتن در این محل به محض روشن شدن کامپیوتر و اجرای یک برنامه آلوده به ویروس و یا دسترسی به رکورد راه انداز ، همراه آن در حافظه اصلی جا می گیرند و بعضی از آنها تا موقع خاموش شدن کامپیوتر همانجا باقی مانده و فایل های دیگر را آلوده می کنند، حتی اگر برنامه آلوده را حذف کرده یا فلاپی دیسک آلوده را نیز از دیسک گردان بیرون آورید.

رکورد راهانداز (Boot Record)

اولین سکتور یک دیسک است که در این سکتور توضیحاتی در مورد دیسک از قبیل ساین سکتورهای دیسک ، ساین کلاسترها و ... قرار دارد. علاوه بر این اطلاعات ، در دیسک های راهانداز این سکتور شامل برنامه ای است که سیستم عامل را در حافظه قرار داده و آن را راهاندازی می کند.

۴-۱-۲ ویروسهای تاثیرگذار بر روی جدول Partition

عملکرد ویروسهای تاثیرگذار بر روی جدول Partition همانند ویروسهای تاثیر گذار بر روی رکورد راهانداز هستند. این ویروس ها علاقه خاصی به پنهان شدن در جدول Partition دارند زیرا جدول Partition شامل اطلاعات تقسیم بندی دیسک سخت است که در سکتور شماره صفر دیسک سخت قرار دارد. اینگونه از ویروسها با قرار گرفتن در این محل به محض روشن شدن کامپیوتر و اجرای یک برنامه آلوده به ویروس و یا دسترسی به جدول Partition آلوده، همراه آن نرم افزار در حافظه اصلی جا می گیرند و گاهی اوقات تا موقع خاموش شدن کامپیوتر همانجا باقی مانده و فایل های دیگر را آلوده می کنند. همچنین ویروس هایی یافت می شوند که اطلاعات مربوط به Setup سیستم را نیز خراب کرده یا تغییر می دهند.

۲-۲ روشهای انتقال ویروس

ویروس های کامپیوتری ممکن است از راه های زیر به کامپیوتر انتقال یابند :

۱-۲-۲ انتقال ویروس از طریق دیسکت یا سی دی آلوده

بعضی از ویروس ها با چسبیدن به انتهای فایل های اجرایی (با پسوند EXE و COM) یا با قرار گرفتن روی سکتور دیسکت خود را به روی کامپیوتر منتقل می کنند. با اجرای فایل های آلوده یا با قرار دادن



دیسکت آلوده در کامپیوتر و استفاده از آن، ویروس به کامپیوتر منتقل شده و فعالیت خود را آغاز می‌کند.

۲-۲-۲ انتقال ویروس از طریق شبکه

هرگاه یکی از کامپیوترهای متصل به شبکه آلوده به ویروس باشد، ممکن است ویروس از طریق شبکه همه کامپیوترها را آلوده نماید. بعضی از ویروس‌ها مخصوص شبکه هستند و ابتدا کامپیوتر سرویس دهنده (Server) را آلوده می‌کنند و سپس توسط کامپیوتر سرویس‌دهنده، کلیه کامپیوترهای شبکه را آلوده می‌سازند.

۲-۲-۳ انتقال ویروس از طریق اینترنت

با گسترش استفاده از اینترنت، ویروس‌های اینترنتی به عنوان نسل جدیدی از ویروس‌ها مطرح شدند. ویروس‌های اینترنتی بسیار سریعتر از ویروس‌های دیگر در سطح دنیا انتشار می‌یابند، به صورتیکه ظرف چند روز میلیون‌ها کامپیوتر در سراسر دنیا به یک ویروس جدید آلوده می‌شوند. این نوع ویروس‌ها ممکن است از طریق پست الکترونیک و یا از طریق دریافت فایل از اینترنت و ... به کامپیوتر منتقل شوند.



- ۱ - انواع ویروس از نظر محل تاثیر گذاری را نام ببرید.
- ۲ - عملکرد ویروس‌های تاثیر گذار بر روی فایل‌های اجرایی را شرح دهید.
- ۳ - عملکرد ویروس‌های تاثیر گذار بر روی فایل‌های غیر اجرایی را شرح دهید.
- ۴ - عملکرد ویروس‌های تاثیر گذار بر رکورد راه‌انداز را شرح دهید.
- ۵ - عملکرد ویروس‌های تاثیر گذار بر جدول Partition را شرح دهید.
- ۶ - روش‌های انتقال ویروس به کامپیوتر را نام ببرید.



۱- کدامیک از گزینه‌های زیر برای جایگیری ویروسها محبوب نیست؟

الف) فایل‌های اجرایی

ب) رکورد راه‌انداز و فایل‌های غیر اجرایی

ج) جدول راه‌انداز

د) جدول پارتیشن

۲ - انتقال از روش‌های انتقال ویروس می‌باشد.

الف) از طریق دیسک آلوده

ب) از طریق CD آلوده

ج) از طریق شبکه و اینترنت

د) هر سه گزینه

۳ - کدام یک از روش‌های انتقال، ویروس را سریعتر منتشر می‌کند؟

الف) از طریق اینترنت

ب) از طریق CD آلوده

ج) از طریق دیسک آلوده

د) از طریق شبکه



فصل	سؤال	الف	ب	ج	د
دوم	۱			✓	
	۲				✓
	۳	✓			

توانایی سوم

تشخیص ویروسی شدن سیستم

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ☒ راههای تشخیص ویروسی شدن سیستم را نام ببرد.
- ☒ علائم ویروسی شدن سیستم را نام ببرد.
- ☒ کند شدن سیستم و دلایل آن شرح دهد.
- ☒ عدم راهاندازی سیستم و دلایل آن را شرح دهد.
- ☒ عدم اجرا شدن فایل های اجرایی و دلایل آن را شرح دهد.
- ☒ کند شدن ارتباط با اینترنت و دلایل آن را شرح دهد.

زمان نظری : ۱ ساعت

زمان عملی : _____



۳-۱ اصول تشخیص ویروسی شدن سیستم

ارائه روش دقیق و مشخصی برای تشخیص ویروسی بودن کامپیوتر امکان پذیر نیست اما از آنجاییکه همه ویروس‌ها درصدد ایجاد مزاحمت و اختلال در کار کامپیوتر هستند و عملکرد همه آنها منفی می‌باشد، لذا می‌توان از روی عملکرد آنها و عوارض ناشی از عملکرد آنها، ویروسی شدن سیستم را تشخیص داد. عملکرد ویروس‌ها را که در واقع راه‌هایی جهت تشخیص ویروسی شدن سیستم می‌باشند می‌توان بشرح زیر دسته بندی کرد :

- ایجاد تاخیر، وقفه یا اختلال در عملیات راه اندازی کامپیوتر یا اجرای برنامه‌ها و فایل‌های اجرایی.

- تخریب یا حذف اطلاعات و برنامه‌ها و یا حتی فرمت کردن دیسک‌ها.

- اشغال حافظه و تکثیر در حافظه بطوریکه جایی برای اجرای برنامه های دیگر وجود نداشته باشد.

مزاحمت‌ها و اختلال‌های فوق ممکن است به محض فعال شدن ویروس انجام شوند.

بطور کلی علائم زیر می‌تواند نشان‌دهنده ویروسی شدن کامپیوتر باشد :

۳-۱-۱ کند شدن سیستم

البته هر نوع کند شدن سیستم را نمی‌توان به ویروس‌ها مرتبط کرد. کند شدن سیستم ممکن است به علت اجرای برنامه‌های متعدد، کم بودن حافظه اصلی کامپیوتر ، پایین بودن مشخصات کامپیوتر و ... باشد. ولی اگر کامپیوتر شما قبلاً با همین وضعیت سرعت مناسبی داشته و هم‌اکنون سرعت اجرای برنامه‌ها کم شده ، ممکن است سیستم شما ویروسی شده باشد.

۳-۱-۲ اشکال در راه‌اندازی سیستم

اگر هنگام راه‌اندازی کامپیوتر ، مشکلی پیش آید و کامپیوتر راه‌اندازی نشود، ممکن است کامپیوتر ویروسی شده باشد. معمولاً این ویروس‌ها بر روی سکتور صفر دیسک سخت قرار می‌گیرند. بعضی از این ویروس‌ها هنگام راه‌اندازی سیستم پیغامی را نمایش می‌دهند و به کاربر اعلام می‌کنند که کامپیوتر ویروسی است. یکی از این ویروس‌ها ، ویروس **One Half** است که در هنگام راه‌اندازی کامپیوتر، عبارت زیر را نمایش می‌دهد :

This is One Half ...



۳-۱-۳ اشکال در اجرای فایل‌های اجرایی

اگر فایل‌های اجرایی کامپیوتر، دچار مشکل شوند و اجرا نشوند ممکن است این فایل‌ها به ویروس آلوده شده باشند. گاهی اوقات وقتی یک فایل اجرایی به ویروس آلوده می‌شود، اندکی اندازه آن افزایش پیدا می‌کند. ولی ویروس‌هایی هم هستند که بدون آنکه اندازه یک فایل را تغییر دهند، آن را آلوده می‌کنند.

۳-۱-۴ کند شدن ارتباط با اینترنت

بعضی از ویروس‌ها، اطلاعات کامپیوتر ما را بصورت مخفیانه از طریق اینترنت به نویسنده ویروس ارسال می‌کنند. بعضی از ویروس‌ها ممکن است از طریق اینترنت خود را تکثیر کنند. یعنی پس از متصل شدن کامپیوتر به اینترنت شروع به تکثیر خود در اینترنت نمایند. بنابراین کند شدن ارتباط با اینترنت نیز می‌تواند یکی از دلایل ویروسی شدن کامپیوتر باشد.



۱ - راههای تشخیص ویروسی شدن سیستم را نام ببرید.

۲ - علائم ویروسی شدن سیستم را نام ببرید.

۳ - کند شدن سیستم و دلایل آن شرح دهید.

۴ - عدم راهاندازی سیستم و دلایل آن را شرح دهید.

۵ - عدم اجرا شدن فایل‌های اجرایی و دلایل آن را شرح دهید.

۶ - کند شدن ارتباط با اینترنت و دلایل آن را شرح دهید.



۱ - کدامیک از علائم زیر نشانه ویروسی شدن سیستم نیست؟

الف) ایجاد تاخیر، وقفه یا اختلال در عملیات راه اندازی کامپیوتر یا اجرای برنامه‌ها و فایل‌های اجرایی.

ب) توقف عملیات نرم‌افزار

ج) تخریب یا حذف اطلاعات و برنامه‌ها و یا حتی فرمت کردن دیسکها.

د) اشغال حافظه و تکثیر در حافظه بطوریکه جایی برای اجرای برنامه های دیگر وجود نداشته باشد.

۲ - کند شدن کامپیوتر از علائم است.

الف) اجرای برنامه‌های متعدد

ب) کم بودن حافظه اصلی کامپیوتر

ج) ویروسی شدن

د) هر سه مورد

۳ - اگر هنگام راه‌اندازی کامپیوتر مشکلی پیش آید یا پیغامی نظیر **This is one Half** نمایش

داده شود، نشانه چیست؟

الف) اجرای برنامه‌های متعدد

ب) کم بودن حافظه اصلی کامپیوتر

ج) ویروسی شدن

د) هر سه مورد



فصل	سوال	الف	ب	ج	د
سوم	۱		✓		
	۲				✓
	۳			✓	

توانایی چهارم

مقابله با ویروسی شدن سیستم

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ☒ روشهای مقابله با ویروسی شدن سیستم را نام ببرد.
- ☒ ویروس اینترنتی را شرح دهد.
- ☒ روشهای انتشار ویروسهای اینترنتی را نام ببرد.
- ☒ روشهای مقابله با ویروسهای اینترنتی را شرح دهد.
- ☒ نحوه پاکسازی ویروسهای مقیم در حافظه را شرح دهد.
- ☒ نحوه پاکسازی ویروسهای غیر مقیم در حافظه را شرح دهد.
- ☒ نحوه پاکسازی ویروسهای اینترنتی را شرح دهد.
- ☒ نرمافزار ضد ویروس را تعریف کند و با چند نمونه از آنها آشنا باشد.
- ☒ روشهای مقابله نرمافزارهای ضد ویروس با ویروسها را شرح دهد.

زمان نظری : ۲ ساعت

زمان عملی : ۴ ساعت



۴-۱ روشهای مقابله با ویروسها

در علوم پزشکی معروف است که پیشگیری آسانتر از درمان است در خصوص ویروسهای کامپیوتری نیز همین جمله کاملاً مصداق دارد، بطور کلی راههای اصلی مقابله و مبارزه با ویروسها به دو دسته زیر تقسیم می شوند :

- شناسائی ویروس ها و جلوگیری از ورود آنها به کامپیوتر (پیشگیری).
- از بین بردن ویروس های وارد شده به کامپیوتر و در صورت لزوم به وضعیت عادی بر گرداندن وضعیت سیستم (درمان).
- بعضی از راههای مقابله با ویروسی شدن سیستم عبارتند از :
 - ویروس ها هنگام ورود به سیستم به ناچار باید روی حافظه، برنامه و یا ناحیه سیستمی دیسک قرار گیرند لذا معمولاً در سیستم یک حالت نوشتن اطلاعات بوجود می آید که این عمل تا حدودی قابل کنترل است. مثلاً با Write Protected کردن فلاپی دیسک یا Read Only کردن پارتیشن های دیسک می توان از نوشتن جلوگیری کرد. (پیشگیری)
 - حتی المقدور از اتصال به کامپیوترها و شبکه هایی که از عدم ویروسی بودن آنها اطمینان ندارید بپرهیزید. (پیشگیری)
 - هرگز از فلاپی دیسک هایی که از عدم ویروسی بودن آنها اطمینان ندارید استفاده نکنید. (پیشگیری)
 - روی سیستم خود حتماً برنامه های ضد ویروسی که قابلیت مقیم شدن در حافظه را دارند قرار دهید. (پیشگیری)
 - تنظیمات مربوط به کنترل ویروس را در Setup سیستم خود انجام دهید. (پیشگیری)
 - وقتی ویروسی بر روی ناحیه سیستمی دیسک یا بر روی فایل برنامه می نشیند، اندازه، تاریخ یا بعضی دیگر از مشخصات فایل اجرایی را تغییر می دهد. لذا می توان با تهیه Backup های مرتب و مقایسه مشخصات فایل های اجرایی و برنامه ها با نسخه های قبلی آنها از وجود احتمالی ویروس آگاهی پیدا کرد. (درمان)



۲-۴ روشهای مقابله با ویروسهای اینترنتی

با گسترش شبکه اینترنت، ویروسها راه مناسب و سریعتری را برای گسترش و تکثیر خود پیدا کردند بصورتی که اکثر ویروسهای امروزی از طریق اینترنت منتقل می‌شوند.

ویروس اینترنتی

ویروسهای اینترنتی به آن دسته از ویروسهای کامپیوتری اطلاق می‌شود که از طریق اینترنت تکثیر یافته و منتقل می‌شوند.

ویروسهای اینترنتی اغلب از طرق زیر وارد کامپیوتر می‌شوند:

- انتقال از طریق نامه‌های الکترونیکی (E-mail)

به همراه نامه‌های الکترونیکی می‌توان فایل‌هایی را به صورت ضمیمه ارسال نمود. این فایل‌های ضمیمه ممکن است حاوی ویروس باشند. متأسفانه نامه‌های الکترونیکی بدون ضمیمه نیز می‌توانند حاوی ویروس باشند. به علت ضعفهای امنیتی نرم‌افزارهای دریافت نامه‌های الکترونیکی نظیر نرم‌افزار Outlook Express ممکن است نامه‌های بدون ضمیمه نیز مخرب باشند. از معروفترین و خطرناکترین ویروسهای اینترنتی که از طریق نامه‌های الکترونیکی انتقال می‌یابد، می‌توان به ویروس NIMDA اشاره کرد. این ویروس در عرض چند روز میلیونها کامپیوتر را در سراسر دنیا آلوده کرد و متأسفانه هنوز هم مواردی از آلودگی به این ویروس مشاهده می‌شود.

- انتقال از طریق دریافت فایل آلوده از اینترنت

ممکن است در صفحات وب فوق متن دریافت فایل‌های اجرایی وجود داشته باشد. که با کلیک کردن این فوق‌متن‌ها، یک فایل اجرایی و یا یک سند از طریق اینترنت دریافت شود. این فایل‌ها ممکن است به ویروس‌ها آلوده باشند. در اینترنت سایتهایی وجود دارد که نرم‌افزارهای قفل شکسته را به صورت رایگان در اختیار افراد قرار می‌دهند. ممکن است این نرم‌افزارها آلوده به ویروس باشد.



بهترین راه مبارزه با ویروسهای اینترنتی، پیشگیری از آلوده شدن به اینگونه ویروسهاست. برای جلوگیری از آلوده شدن به ویروسهای اینترنتی به توصیههای ساده اما مهم زیر توجه کنید :

- نامه‌های الکترونیکی مشکوک را باز نکنید.
- ضمیمه‌های نامه‌های الکترونیکی ناشناس را باز نکنید.
- اگر ضمیمه نامه‌ها، فایل‌های اجرایی یا اسناد نرم‌افزارهایی نظیر Microsoft Word بود بدون بررسی توسط نرم‌افزارهای ضد ویروس آنها را اجرا نکنید.
- فایل‌ها و برنامه‌هایی که از اینترنت دریافت می‌کنید، حتماً با نرم‌افزارهای ضد ویروس بررسی کرده و پس از اطمینان از سالم بودن فایل‌های دریافتی ، از آنها استفاده نمایید.
- نرم‌افزارهای ویروس یاب خود را به موقع بروز رسانی نمایید.
- سیستم‌عامل و نرم‌افزارهای اینترنتی خود را به موقع بروز رسانی نمایید.
- همواره از اخبار ویروس‌های جدید مطلع باشید. سایتهای مفیدی در این زمینه وجود دارند که آخرین اطلاعات ویروس‌های جدید را برای شما ارسال می‌کنند. این اطلاعات که به صورت نامه الکترونیکی برای شما ارسال می‌شود، حاوی اطلاعاتی در مورد نحوه شناسایی ویروس و فعالیتهای که ویروس انجام می‌دهد و نحوه حذف آن است. تعدادی از این سایتها عبارتند از:

<http://www.mcafee.com> و <http://www.antivirus.com/vinfo>

۳-۴ آشنایی با مراحل پاکسازی سیستم آلوده

در صورتیکه به هر دلیلی کامپیوتر ما به ویروس آلوده شد ، باید هر چه سریعتر برای پاکسازی آن اقدام کنیم. برای پاکسازی ویروسها نمی‌توان یک روش مشخص را تعیین کرد زیرا هر ویروس عملکرد خاصی دارد که با توجه به نحوه تاثیرگذاری ویروس ، نوع ویروس ، نحوه آلوده کردن سیستم و ... باید روش مناسبی را جهت پاکسازی ویروس انتخاب کرد. ما در این قسمت پاکسازی ویروسها را به سه روش کلی توضیح می‌دهیم که هر روش برای پاکسازی ویروسهای خاصی کاربرد دارد.



۴-۳-۱ پاکسازی ویروسهای مقیم در حافظه

ویروسهای مقیم در حافظه، اغلب ویروسهایی هستند که بر روی رکورد راهانداز یا جدول **Partition** قرار دارند و در هنگام راهاندازی کامپیوتر فعال شده و در حافظه باقی می‌مانند. تا هنگامی که این ویروسها در حافظه قرار دارند، نمی‌توان برای پاکسازی آنها اقدام نمود.

جهت پاکسازی این نوع ویروسها مراحل زیر را انجام می‌دهیم :

- ☒ در صورت روشن بودن کامپیوتر، آن را مجدداً راهاندازی می‌نماییم.
- ☒ کامپیوتر را با یک دیسکت یا **CD** راهانداز سالم و عاری از ویروس ، راهاندازی می‌کنیم.
- ☒ دیسکت یا **CD** ضد ویروس مناسب را در درایو قرار داده و ویروسها را پاکسازی می‌نماییم.
- ☒ در صورتیکه سیستم عامل کامپیوتر آسیب دیده است و یا سیستم راهاندازی نمی‌شود می‌باید با توجه به نوع سیستم عامل ، عملیات بازسازی و احیاء سیستم عامل انجام شود.

۴-۳-۲ پاکسازی ویروسهای غیر مقیم در حافظه

از آنجایی که این ویروسها در حافظه فعال نیستند، کفایت با نرم‌افزار ضدویروس مناسب آنها را پاکسازی نماییم.

جهت پاکسازی این نوع ویروسها مراحل زیر را انجام می‌دهیم :

- ☒ دیسکت یا **CD** ویروس یاب مناسب را در درایو قرار داده و ویروسها را پاکسازی می‌نماییم.

۴-۳-۳ پاکسازی ویروسهای اینترنتی

همانطور که می‌دانیم ویروسهای اینترنتی ، از طریق اینترنت به کامپیوتر منتقل می‌شوند. پس هنگام پاکسازی این ویروسها باید اتصال به اینترنت را قطع نمود زیرا ممکن است بلافاصله پس از پاکسازی ویروس، کامپیوتر مجدداً آلوده شود.

جهت پاکسازی این نوع ویروسها مراحل زیر را انجام می‌دهیم :

- ☒ ارتباط با اینترنت را قطع می‌کنیم.
- ☒ با توجه به دستورالعمل پاکسازی ویروس ، ممکن است نیاز باشد کامپیوتر را مجدداً راهاندازی می‌کنیم.
- ☒ دیسکت یا **CD** ضد ویروس مناسب را در درایو قرار داده و ویروسها را پاکسازی می‌نماییم.



۴-۴ آشنایی با نرم افزارهای ضد ویروس

یکی از روشهای جلوگیری از انتقال ویروس به کامپیوتر و حذف ویروسها از کامپیوتر استفاده از نرم افزارهای ضد ویروس است. نرم افزارهای ضد ویروس نرم افزارهایی هستند که فایل های آلوده به ویروس را شناسایی کرده و ویروس را از روی کامپیوتر حذف می کنند.

همانطوریکه می دانید همه روزه ویروس های جدید با ساختار و عملکردهای مختلف توسط ویروس نویسان ساخته می شوند که شناسایی ساختار و عملکرد آنها و تهیه برنامه های ضد ویروس مناسب آنها، مستلزم صرف هزینه و وقت نسبتاً زیادی است. به همین دلیل تهیه ضد ویروس مناسب هر ویروس، براحتی امکان پذیر نیست و هیچ شرکت تولید کننده برنامه های ضد ویروس، نمی تواند ادعا نماید که قادر به شناسایی و از بین بردن تمام ویروس ها می باشند و تا زمانیکه ضد ویروس یک ویروس جدید طراحی می گردد ممکن است کامپیوترهای زیادی آلوده و دچار اختلال گردند. از معروفترین و متداولترین نرم افزارهای ضد ویروس می توان به نرم افزارهای زیر اشاره کرد:

- McAfee Virus Scan
- Norton Antivirus
- Panda Antivirus
- Dr Web

نرم افزارهای ضد ویروس فقط می توانند ویروسهای شناخته شده را تشخیص دهند و قادر نیستند ویروسهای جدید را تشخیص دهند. برای حل این مشکل ، در نرم افزارهای ضد ویروس امکان بروز رسانی در نظر گرفته شده است به صورتیکه از طریق اینترنت می توان نرم افزار ضد ویروس را بروز رسانی کرد. شرکتهای تولید کننده نرم افزارهای ضد ویروس جدیدترین ویروسها را شناسایی کرده و فایل های بروز رسانی نرم افزار ضد ویروس خود را در سایت وب قرار می دهند تا مشترکین آنها در سراسر دنیا نرم افزارهای خود را بروز رسانی نمایند.

۴-۵ روشهای مقابله نرم افزارهای ضد ویروس با ویروسها

نرم افزارهای ضد ویروس به روش های زیر با ویروسها مقابله می کنند :

- پیشگیری از آلوده شدن به ویروس

در هنگام وارد شدن ویروس به کامپیوتر ، پیغام هشدار دهنده ای را به کاربر نمایش می دهند و از فعال شدن ویروس خودداری می کنند.



- پاک کردن ویروس

فایلهای سالمی که به ویروس آلوده شده اند را شناسایی می کنند و در صورت امکان آنها را ویروس زدایی کرده و به صورت اولیه باز می گردانند به این عمل **disinfecting** (ویروس زدایی) می گویند.

- قرنطینه کردن فایل ویروسی

در صورتیکه نتوانند یک فایل آلوده را ویروس زدایی کنند آن فایل را قرنطینه کرده و به کاربر اطلاع می دهند که این فایل آلوده به ویروس است و امکان ویروس زدایی آن نیست و فعلاً در قرنطینه است. در صورتیکه کاربر مایل باشد می تواند این فایل را به کلی حذف کند. همچنین نرم افزارهای ضد ویروس به کاربران اجازه می دهند، فایل های مشکوک را به قسمت قرنطینه منتقل کنند.



- ۱ - روشهای مقابله با ویروسی شدن سیستم را نام ببرید.
- ۲ - ویروس اینترنتی را شرح دهید.
- ۳ - روش‌های انتشار ویروس‌های اینترنتی را نام ببرید.
- ۴ - روشهای مقابله با ویروس‌های اینترنتی را شرح دهید.
- ۵ - نحوه پاکسازی ویروس‌های مقیم در حافظه را شرح دهید.
- ۶ - نحوه پاکسازی ویروس‌های غیر مقیم در حافظه را شرح دهید.
- ۷ - نحوه پاکسازی ویروس‌های اینترنتی را شرح دهید.
- ۸ - نرم‌افزار ضد ویروس را تعریف کرده و چند نمونه از آنها را نام ببرید.
- ۹ - روش‌های مقابله نرم‌افزارهای ضد ویروس با ویروس‌ها را شرح دهید.



- ۱ - کدامیک از موارد زیر، پیشگیری از ویروسی شدن کامپیوتر می باشد.
- الف) شناسایی ویروس و جلوگیری از ورود آن به کامپیوتر
ب) از بین بردن ویروس وارد شده به کامپیوتر
ج) عدم اتصال به اینترنت
د) هر سه گزینه
- ۲ - برای جلوگیری از ویروسی شدن کامپیوتر چه کاری را باید انجام داد؟
- الف) Write Protected کردن فلاپی دیسک
ب) عدم اتصال به کامپیوترها و شبکه های ناشناخته
ج) عدم استفاده از فلاپی دیسک های ناشناخته
د) هر سه گزینه
- ۳ - ویروس های از طریق نامه های الکترونیکی وارد کامپیوتر می شوند.
- الف) اینترنتی
ب) سیستمی
ج) مخرب
د) مقیم در حافظه
- ۴ - برای جلوگیری از آلوده شدن به ویروس های اینترنتی کدامیک از روش های زیر موثر است؟
- الف) باز نکردن نامه های الکترونیکی مشکوک
ب) بروزرسانی نرم افزار ویروس یاب
ج) بروزرسانی سیستم عامل
د) هر سه مورد



۵ - کدامیک از سایتهای زیر مربوط به برنامههای ضد ویروس می باشند؟

الف) <http://www.mcafee.com> ب) <http://www.antivirus.com>

ج) <http://www.google.com> د) الف و ب

۶ - روشهای مقابله نرم افزارهای ضد ویروس با ویروس ها است.

الف) پیشگیری از آلوده شدن به ویروس

ب) پاک کردن ویروس

ج) قرنطینه کردن فایل ویروسی

د) هر سه مورد

۷ - در صورتیکه دیسکتی که احتمالا حاوی ویروس است به شما داده شده است و شما نیاز

دارید که از این دیسکت استفاده نمایید ، برای اینکه کامپیوتر شما ویروسی نشود چه کاری

باید بکنید؟

الف) دیسکت را فرمت می کنیم.

ب) ابتدا دیسکت را ویروسیابی کرده و پس از حذف ویروسها از آن استفاده می کنیم.

ج) ابتدا دیسکت را Write Protect کرده و پس از حذف ویروسها از آن استفاده می کنیم.

د) گزینه های ب و ج

۸ - فرض کنید که بر روی یک دیسکت چند فایل قرار داده اید و می خواهید این فایلها را در

کامپیوتر دوست خود کپی کنید. با توجه به اینکه کامپیوتر دوست شما ممکن است ویروسی

باشد چه کاری باید انجام دهید تا دیسکت شما ویروسی نشود؟

الف) دیسکت را فرمت می کنیم.

ب) ابتدا دیسکت را از حالت Write Protect خارج کرده و سپس آن را در درایو کامپیوتر

قرار می دهیم.

ج) ابتدا دیسکت را در حالت Write Protect قرار داده و سپس آن را در درایو کامپیوتر قرار

می دهیم.

د) هیچکدام



دستور کار آزمایشگاه



۱ - از طریق اینترنت به سایت <http://www.mcafee.com> متصل شوید و اطلاعاتی در مورد نرم افزار ضد ویروس McAfee بدست آورید.

۲ - از طریق اینترنت به سایت <http://www.antivirus.com> متصل شوید و اطلاعاتی در مورد ویروس های جدید اینترنتی بدست آورید.

۳ - به سایت متصل شوید . در این سایت اطلاعاتی در مورد ویروس های اینترنتی به زبان فارسی وجود دارد. نحوه عملکرد و نحوه مقابله با ویروس های Nimda ، Sircam ، Code Red را بدست آورید.

۴ - عملیات پاکسازی ویروس های مقیم در حافظه را یکبار تمرین کنید.

۵ - عملیات پاکسازی ویروس های غیرمقیم در حافظه را یکبار تمرین کنید.

۶ - عملیات پاکسازی ویروس های اینترنتی را یکبار تمرین کنید.



فصل	سؤال	الف	ب	ج	د
چهارم	۱	✓			
	۲			✓	
	۳	✓			
	۴			✓	
	۵			✓	
	۶			✓	
	۷		✓		
	۸			✓	

توانایی پنجم

کار با نرم افزار ضد ویروس McAfee

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ✓ نرم افزار McAfee را نصب نماید.
- ✓ قسمت های مختلف نرم افزار McAfee را نام برده و کاربرد هر یک را توضیح دهد.
- ✓ عملیات ویروس یابی را به کمک نرم افزار McAfee انجام دهد.
- ✓ نرم افزار McAfee را از طریق اینترنت بروزرسانی نماید.

زمان نظری : ----

زمان عملی : ۴ ساعت



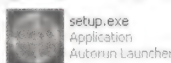
۵-۱ آشنایی با نرم افزار McAfee

با ادغام دو شرکت Dr Solomon's Software (تولیدکننده نرم افزارهای ضد ویروس Toolkit) و شرکت Network Associates (تولیدکننده نرم افزارهای ضد ویروس McAfee) نسل جدیدی از نرم افزارهای پیشرفته ضد ویروس به بازار عرضه شد. در واقع ضد ویروس McAfee ترکیبی از قدرت شناسایی و پاکسازی Toolkit و راحتی استفاده McAfee است. هم اکنون ضد ویروس McAfee بیش از ۷۰ میلیون کاربر در سطح دنیا دارد و در حدود ۵۶٪ بازار نرم افزارهای ضد ویروس در اختیار این ضد ویروس است. از مهمترین مزایای این ضد ویروس، به روزرسانی ساده و سریع آن است. ما در این کتاب نسخه ۲۰۰۴ نرم افزار McAfee را توضیح خواهیم داد. با نحوه نصب و استفاده از این نرم افزار در ادامه همین فصل آشنا می شویم.

۵-۲ نصب نرم افزار McAfee

جهت نصب نرم افزار McAfee عملیات زیر را انجام می دهیم :

☒ **CD نصب نرم افزار McAfee را در درایو قرار داده و فایل Setup.exe را اجرا می کنیم.**



شکل (۵-۱) آیکن برنامه Setup نرم افزار McAfee

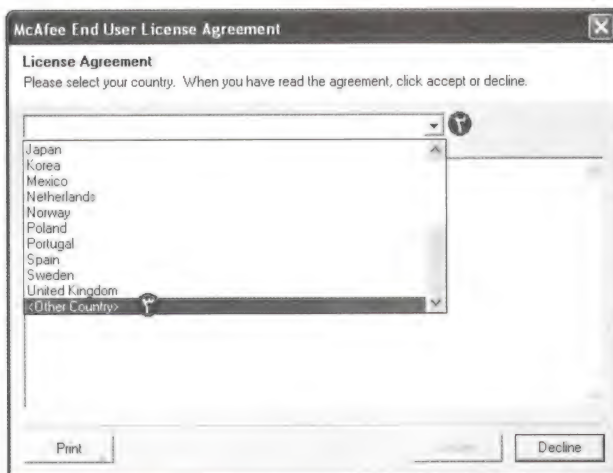
☒ **پنجره ای مطابق شکل زیر ظاهر می شود. در این پنجره بر روی Install McAfee VirusScan کلیک می کنیم.**



شکل (۵-۲) پنجره نصب ضد ویروس McAfee

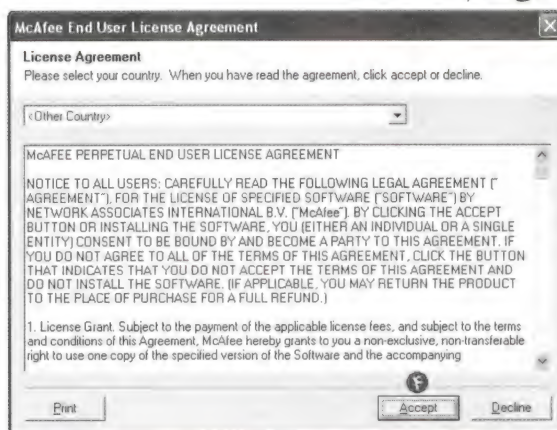


✓ پنجره‌ای مطابق شکل زیر ظاهر می‌شود. در این پنجره از لیست **Country** ، نام کشور خود را انتخاب می‌کنیم. از آنجایی که کشور ایران در این لیست وجود ندارد، گزینه **Other Country** را انتخاب می‌نماییم.



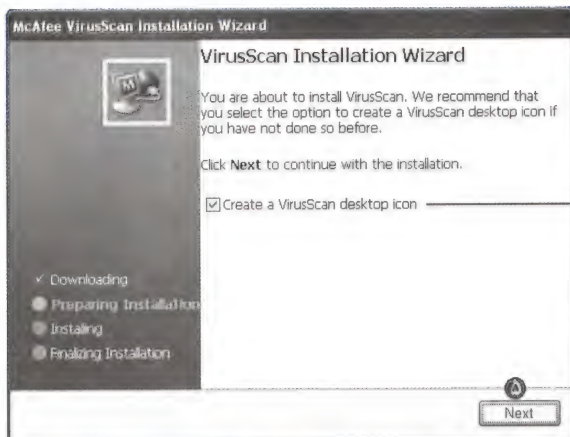
شکل (۳-۵) انتخاب نام کشور - پنجره User License Agreement

✓ متن موافقتنامه مجوز استفاده از نرم‌افزار ظاهر می‌شود. بر روی دکمه **Accept** جهت قبول این موافقت نامه کلیک می‌کنیم.



شکل (۴-۵) نمایش متن موافقتنامه مجوز کاربر نهایی

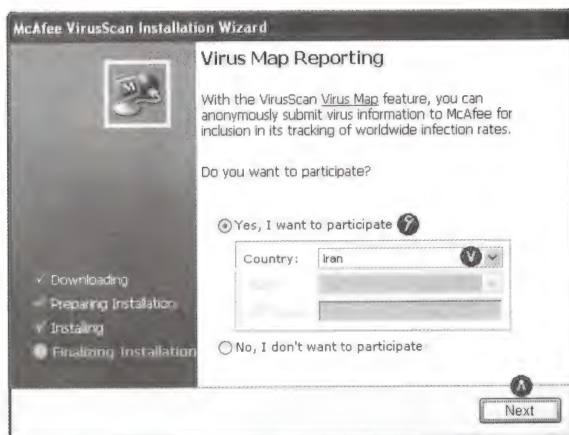
✓ پنجره **VirusScan Installation Wizard** ظاهر می‌شود. در این پنجره می‌توانیم مشخص نماییم که آیا می‌خواهیم برنامه **VirusScan** بر روی میزکار قرار گیرد یا خیر. جهت ادامه کار بر روی دکمه **Next >** کلیک می‌کنیم.



ایجاد آیکن میانه بر
برنامه در میز کار

شکل (۵-۵) پنجره VirusScan Installation Wizard

✓ در مرحله بعد ، برنامه نصب فایل های لازم را بر روی دیسک کپی می کند. سپس پنجره زیر ظاهر می شود. در این پنجره جهت اشتراک داوطلبانه در قسمت **Virus Map** سایت **McAfee** از ما سؤال می شود. به کمک امکان **Virus Map** می توان اطلاعات ویروس های کامپیوتر ما را به صورت ناشناس به شرکت **McAfee** ارسال نمود تا این شرکت بتواند نرخ ابتلا به یک ویروس را در سطح جهان اندازه گیری نماید و آمار کامپیوترهای مبتلا به یک ویروس را در سطح جهان منتشر نماید. در صورتیکه بخواهیم در **Virus Map** مشترک شویم ، گزینه ☒ Yes, I want to participate را انتخاب کرده و نام کشور **Iran** را از لیست انتخاب می نماییم. سپس دکمه را کلیک می کنیم.



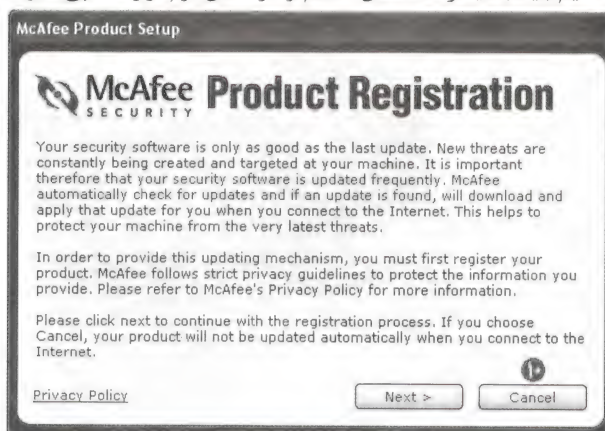
شکل (۵-۶) پنجره Virus Map Reporting

✓ در پنجره بعد دکمه را کلیک می کنیم تا عملیات نصب به پایان برسد.



شکل (۵-۷) پنجره Completing the VirusScan Wizard

✓ پس از این پنجره ، پنجره **Register** کردن نرم افزار **VirusScan** ظاهر می شود. در صورتیکه بخواهیم این پنجره را ببندیم، دکمه **Cancel** را کلیک می کنیم. (در صورتیکه بخواهیم نرم افزار خود را **Register** کنیم باید به اینترنت متصل باشیم و در ضمن نرم افزار ما کی غیرمجاز نباشد).

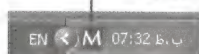


شکل (۵-۸) پنجره McAfee Product Registration

۵-۳ آشنایی با محیط کار نرم افزار McAfee

جهت اجرای نرم افزار McAfee بر روی آیکن **M** که در سینی نوار کار قرار دارد، دوبار کلیک می کنیم.

آیکن نرم افزار McAfee



شکل (۵-۹) آیکن نرم افزار ضد ویروس McAfee در نوار کار ویندوز



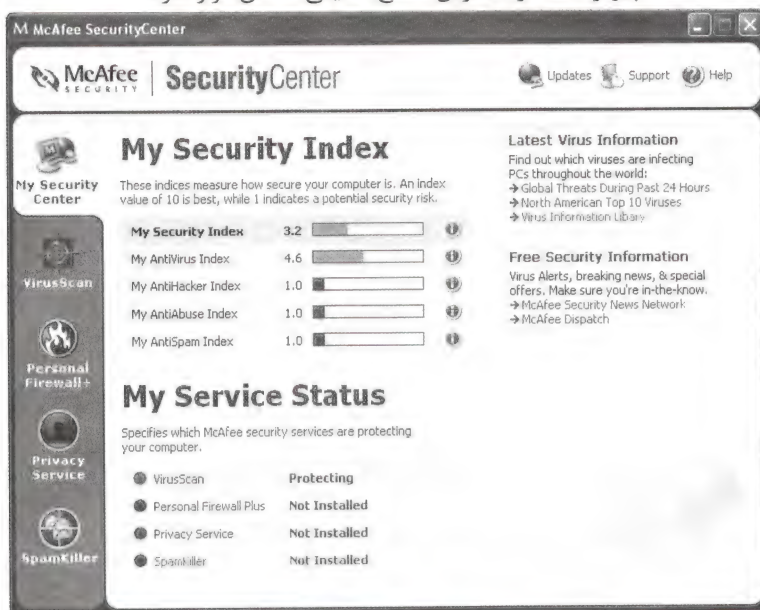
پنجره اصلی برنامه McAfee ظاهر می‌شود. این پنجره شامل چندین سربرگ است که هر سربرگ یک نرم‌افزار جداگانه محسوب می‌شود.

هنگامی که نرم‌افزار McAfee را نصب می‌کنیم، فقط قسمت Virus Scan نصب می‌شود. در ادامه با عملکرد هر یک از سربرگ‌های نرم‌افزار McAfee آشنا خواهیم شد.

My Security
Center

۱-۳-۵ مرکز امنیت

در این سربرگ قسمتی تحت عنوان My Security Index وجود دارد، که در این قسمت ضرابی نمایش داده می‌شود که هر ضریب نشان دهنده میزان امنیت کامپیوتر شما در یک زمینه است. اگر این ضریب یک باشد به این معنی است که امنیت کامپیوتر شما در این موضوع پایین است. ضریب ۱۰ نمایانگر این است که کامپیوتر شما در بالاترین سطح امنیتی ممکن قرار دارد.



شکل (۱۰-۵) سربرگ My Security Center نرم‌افزار McAfee

همانطور که در قسمت My Service Status شکل فوق مشاهده می‌شود، سرویس‌های Personal Firewall، سرویس Privacy Service و Spam Killer بر روی کامپیوتر نصب نشده است. بنابراین ضریب امنیتی این کامپیوتر در این مواد پایین است.



در صورتیکه می‌خواهید ضریب امنیتی کامپیوتر شما در همه زمینه‌ها بالاتر برود باید کارهای زیر را انجام دهید:

- ☒ نرم‌افزار **Virus Scan** خود را از طریق اینترنت بروز کنید.
 - ☒ نرم‌افزار **Personal Firewall** شرکت **McAfee** را نصب نمایید.
 - ☒ سرویس **Privacy Service** شرکت **McAfee** را فعال نمایید.
 - ☒ نرم‌افزار **Spam Killer** شرکت **McAfee** را نصب نمایید.
- با این نرم‌افزارها در ادامه بیشتر آشنا خواهیم شد.



۲-۳-۵ سربرگ ویروس‌یابی

در این سربرگ قسمتهای مختلفی وجود دارد. این قسمتها عبارتند از :

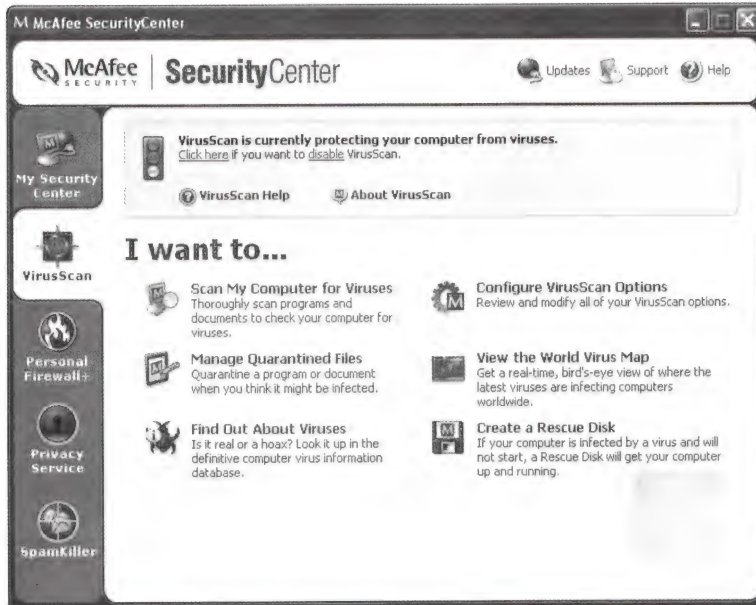
-  **Scan My Computer for Viruses** ویروس‌یابی کامپیوتر من
ویروس‌یابی کامپیوتر و حذف ویروسها از طریق این گزینه انجام می‌گردد.
-  **Configure VirusScan Options** تنظیمات ویروس‌یابی
تنظیمات نرم‌افزار ویروس‌یاب از طریق این گزینه انجام می‌شود.
-  **Manage Quarantined Files** مدیریت فایل‌های قرنطینه شده
قرنطینه کردن برنامه‌ها و اسنادی که تصور می‌کنیم ممکن است ویروسی باشند از طریق این گزینه انجام می‌شود.
-  **View the World Virus Map** مشاهده نقشه جهانی ویروسها
نرم‌افزار **McAfee** اطلاعات آماری ویروسهای مشاهده شده در سراسر جهان را بر روی نقشه از طریق این گزینه در اختیار شما قرار می‌دهد.
-  **Find Out About Viruses** جستجوی اطلاعات ویروسها
در این قسمت می‌توانید اطلاعات کاملی در مورد ویروسهای شناخته شده و نحوه عملکرد و پاکسازی آنها بدست آورید.



Create a Rescue Disk

ایجاد دیسک نجات

این قسمت یک دیسک نجات برای شما می سازد. در صورتیکه کامپیوتر شما ویروسی شود و دیگر راه اندازی نشود، به کمک دیسک نجات می توانید کامپیوتر خود را راه اندازی نمایید.



شکل (۱۱-۵) سربرگ VirusScan نرم افزار McAfee



Personal Firewall+

۳-۵ سربرگ دیوار آتش شخصی

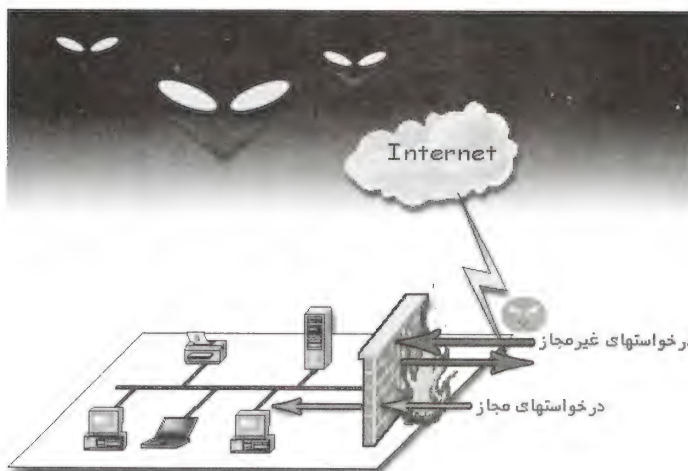
یکی از خطراتی که کامپیوترهای متصل به شبکه های کامپیوتری و شبکه اینترنت را تهدید می کند ، خطر نفوذ افرادی به نام نفوذگر (Hacker) می باشد. نفوذگرها افرادی هستند که از طریق سوراخهای امنیتی موجود در سیستم عامل یا نرم افزارهای دیگر، به کامپیوتر شما نفوذ کرده و علاوه بر اینکه می توانند اطلاعات محرمانه شما را به سرقت ببرند، می توانند آسیبهای جدی به فایل ها و برنامه های شما وارد نمایند. در گذشته، نفوذگرها ، افراد حرفه ای و مسلط به کامپیوتر بودند که معمولاً به کامپیوترهای شرکت های بزرگ و مراکز حساس نفوذ می کردند و کمتر در فکر نفوذ به کامپیوترهای شخصی بودند ولی امروزه با ابزارهای جاسوسی که در سایتهای اینترنتی مخصوص نفوذگرها به رایگان قابل دریافت است، کاربران تازه کار نیز با استفاده از این ابزارها می توانند به راحتی به کامپیوترها نفوذ کنند، بنابراین خطر نفوذ به کامپیوترهای شخصی به مراتب بیشتر شده است. به همین منظور

شرکتهای تولید کننده نرم افزارهای ضد ویروس، به همراه نرم افزار ضد ویروس خود نرم افزاری به نام دیوار آتش (Firewall) نیز ارائه می کنند که این نرم افزار مراقبت از کامپیوتر شما در برابر نفوذگرها را به عهده دارد. در گذشته دیوارهای آتش توسط مدیران شبکه و مسئولین ISP بر روی کامپیوترهای Server نصب می شد ولی امروزه نوع ساده تری از دیوارهای آتش تولید شده اند که به آنها دیوار آتش شخصی (Personal Firewall) می گویند.

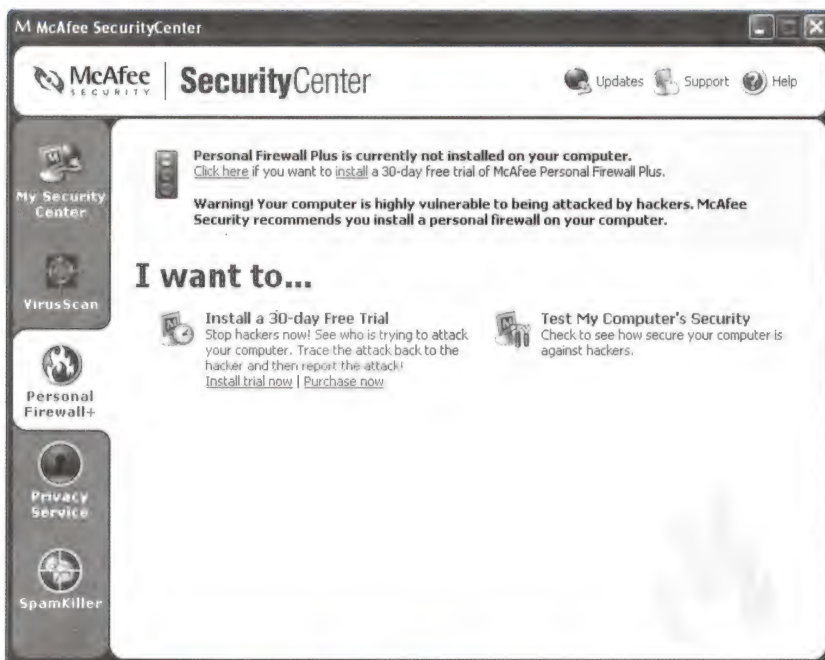
دیوار آتش (Firewall)

سیستم امنیتی را که جهت محافظت از شبکه داخلی در مقابل نفوذ افراد از خارج شبکه طراحی شده است، اصطلاحاً دیوار آتش می گویند.


همانطور که در شکل زیر مشاهده می کنید، دیوار آتش به درخواستهای مجاز اجازه عبور می دهد ولی درخواستهای غیر مجاز را بازمی گرداند و به این ترتیب از نفوذ افراد غیر مجاز جلوگیری می کند.



شکل (۱۲-۵) دیوار آتش به درخواستهای مجاز اجازه عبور می دهد ولی درخواستهای غیر مجاز را بازمی گرداند.



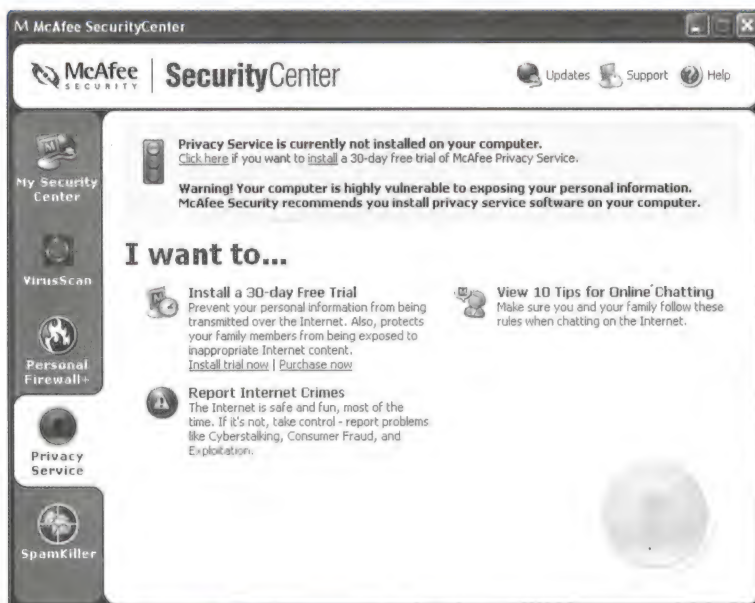
شکل (۱۳-۵) سربرگ Personal Firewall نرم افزار McAfee

همانطور که در شکل مشاهده می کنیم نرم افزار دیوار آتش شخصی، نصب نشده است و برای نصب آن باید بر روی  **Install a 30-day Free Trial** کلیک کنیم تا از طریق اینترنت، نسخه آزمایشی ۳۰ روزه آن بر روی کامپیوتر ما نصب شود.



Privacy
Service

۴-۳-۵ سربرگ سرویس اختفاء
در این سربرگ، نرم افزار McAfee سرویس دیگری را به نام سرویس اختفاء در اختیار کاربران خود قرار می دهد. این سرویس از انتشار اطلاعات شخصی شما در شبکه اینترنت جلوگیری می کند. همچنین توسط این سرویس می توان قوانینی را وضع نمود که دسترسی به سایتهای غیر مجاز غیر ممکن شود.



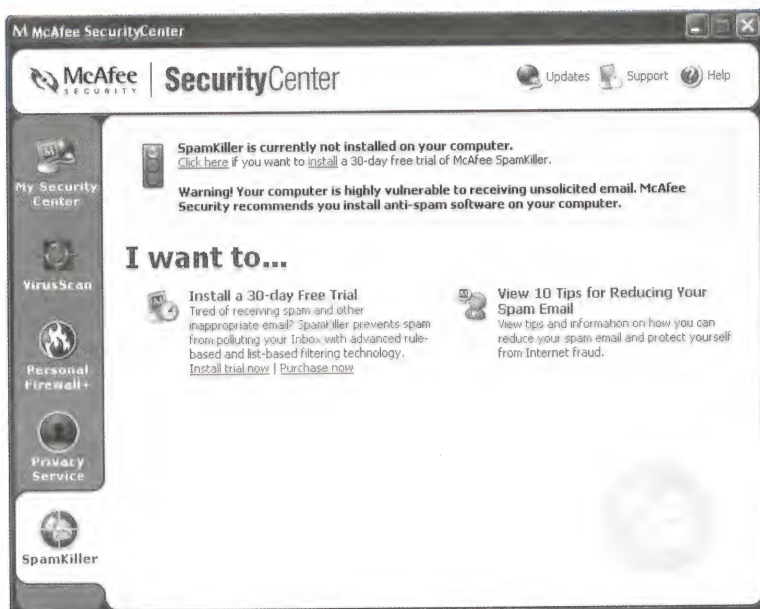
شکل (۱۴-۵) سربرگ Privacy Service



۵-۳-۵ سربرگ نابودکننده هرز نامه

یکی از مشکلاتی که کاربران اینترنتی با آن مواجه هستند، ارسال نامه‌های الکترونیکی زیاد بصورت ناخواسته و معمولاً با محتوای تبلیغاتی است که باعث می‌شود صندوق پستی الکترونیکی افراد مملو از این نامه‌ها شود. به اینگونه نامه‌ها هرزنامه (Spam) گفته می‌شود.

در این سربرگ، امکان نصب نسخه آزمایشی ۳۰ روزه نرم‌افزار SpamKiller قرار داده شده است. این نرم‌افزار نامه‌های Spam را تشخیص داده و از صندوق پست الکترونیک شما حذف می‌کند. در این نرم‌افزار می‌توان قوانینی را وضع کرد که نامه‌های خاصی را به عنوان Spam شناسایی کرده و حذف نماید.





شکل (۵-۱۵) سربرگ SpamKiller نرم‌افزار McAfee

۵-۴ ویروس‌یابی با نرم‌افزار McAfee

پس از نصب نرم‌افزار McAfee، این نرم‌افزار بصورت مقیم در حافظه قرار می‌گیرد. در ضمن هر بار که کامپیوتر را روشن کنیم این نرم‌افزار به صورت خودکار اجرا شده و در حافظه قرار می‌گیرد. هر فایل یا پوشه‌ای را که باز کنیم، نرم‌افزار McAfee بصورت خودکار فایل‌های داخل آن را پوشه را بررسی می‌کند و در صورتیکه فایل ویروسی پیدا کند بلافاصله پیغامی را نمایش می‌دهد و از فعالیت ویروس جلوگیری می‌کند.

گاهی اوقات ممکن است بخواهیم تمام یا بخشی از فایل‌های کامپیوتر را ویروس‌یابی کنیم.
برای ویروس‌یابی کامپیوتر عملیات زیر را انجام می‌دهیم :

☒ بر روی آیکن  در سینی نوار کار، دوبار کلیک می‌کنیم.

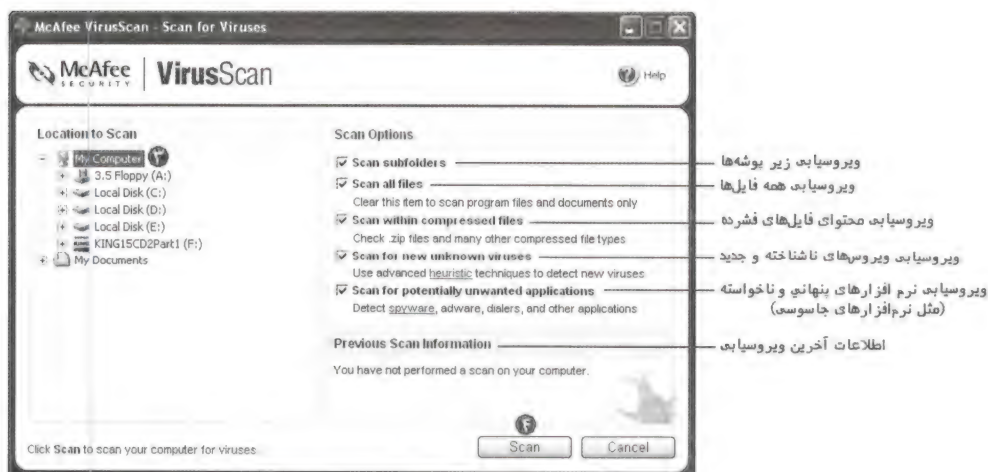
☒ در پنجره برنامه McAfee، روی سربرگ  کلیک می‌کنیم.

☒ در این سربرگ، بر روی  Scan My Computer for Viruses کلیک می‌کنیم.



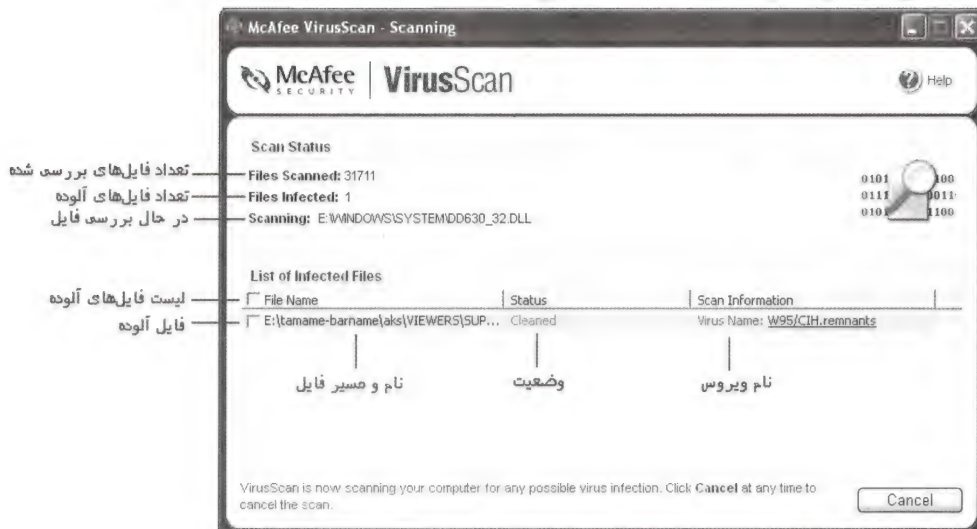
شکل (۱۶-۵) سربرگ VirusScan نرم افزار McAfee

☑ در پنجره ظاهر شده، درایو یا پوشه مورد نظر را جهت ویروس یابی انتخاب می کنیم. همچنین در قسمت *Scan Options* می توان تعیین نمود چگونه ویروس یابی انجام شود.



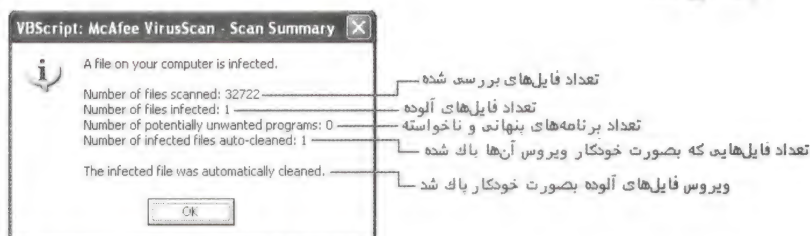
شکل (۱۷-۵) پنجره ویروس یابی - انتخاب پوشه ها و تنظیمات ویروس یابی

✓ برنامه ویروس یاب **McAfee** کلیه فایل ها و برنامه های را مورد بررسی قرار داده و در صورت یافتن ویروس، آن را در لیست پایین پنجره نمایش می دهد. در صورتیکه ویروس قابل پاک شدن باشد، ویروس را از فایل پاک می کند در غیر این صورت فایل ویروسی را قرنطینه می نماید. وضعیت فایل های آلوده در قسمت **Status** مشخص شده است.



شکل (۵-۱۸) پنجره ویروس یابی - عملیات ویروس یابی

✓ در پایان پنجره ای نمایش داده می شود که آماری از فایل های بررسی شده و ویروس های یافت شده ارائه می کند.




شکل (۵-۱۹) پنجره خلاصه ویروس یابی

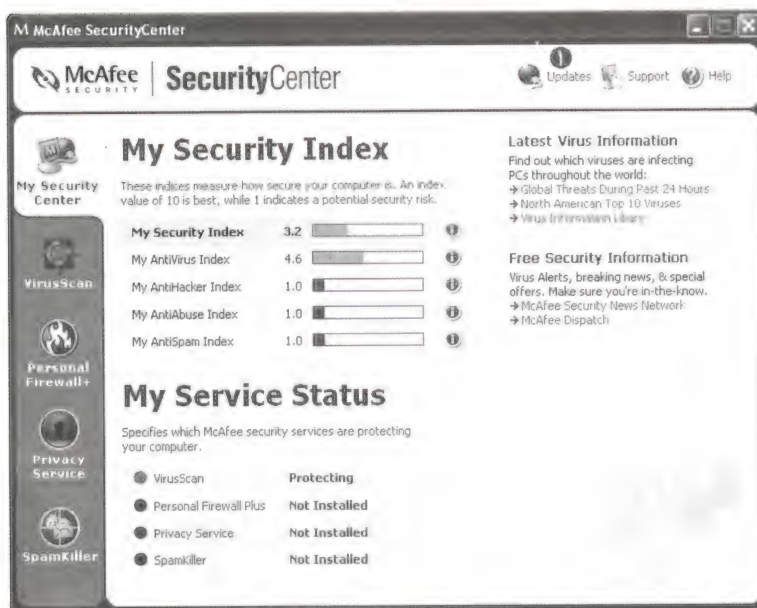
۵-۵ بروزرسانی نرم افزار McAfee

همانطور که می دانیم، ممکن است ظرف یک هفته یا چند روز ویروسهای جدیدی توسط افراد خرابکار تولید شود. نرم افزارهای ضد ویروس فقط قادر به شناسایی ویروسهای شناخته شده هستند بنابراین نیاز است که هر چند روز یکبار آنها را بروزرسانی نماییم. البته نرم افزار ضد ویروس **McAfee** از روشی


استفاده می‌کند که ویروس‌های جدیدی که ساختاری مشابهی با ویروس‌های قدیمی دارند شناسایی می‌کند ولی این نرم‌افزار نیز برای شناسایی ویروس‌های با ساختار جدید نیاز به بروزرسانی دارد. شرکت‌های تولید کننده نرم‌افزارهای ضد ویروس، آخرین ویروس‌های را در سطح دنیا شناسایی می‌کنند و پس از تشخیص عملکرد و نحوه پاک کردن آنها، اطلاعات ویروس و نحوه حذف آن را در سایتهای اینترنتی خود قرار می‌دهند. در ضمن امکان بروزرسانی نرم‌افزارهای ضد ویروس را از طریق اینترنت به کاربران خود می‌دهند.

جهت بروزرسانی نرم‌افزار **McAfee** عملیات زیر را انجام می‌دهیم :

- ☒ ابتدا به اینترنت متصل می‌شویم.
- ☒ بر روی آیکن **M** در سینی نوار کار، دوبار کلیک می‌کنیم.
- ☒ در پنجره اصلی نرم‌افزار **McAfee** بر روی آیکن  کلیک می‌کنیم.



شکل (۲۰-۵) پنجره اصلی نرم‌افزار ضد ویروس **McAfee**

- ☒ در پنجره ظاهر شده توضیح داده شده است که نرم‌افزار **McAfee** بصورت خودکار ، عملیات بروزرسانی را انجام می‌دهد (البته اگر به اینترنت متصل باشیم) در این پنجره بر روی دکمه  کلیک می‌کنیم.



شکل (۵-۲۱) بروزرسانی نرم افزار McAfee

✓ نرم افزار McAfee به سایت وب خود متصل شده و در صورتیکه لازم باشد فایل های **Dat** که حاوی اطلاعات شناسایی و پاک کردن ویروسها هستند را بروزرسانی می نماید. در صورتیکه نسخه جدیدی از نرم افزار McAfee نیز وجود داشته باشد با گرفتن اجازه از شما ، نرم افزار را دریافت و نصب می کند.

شکل (۵-۲۲) بررسی سایت McAfee جهت بروزرسانی نرم افزار و فایل های **Dat**



- ۱ - منظور از ضریب امنیتی کامپیوتر در نرم افزار McAfee چیست؟ ضریب ۱ و ضریب ۱۰ چه معنایی دارند؟
- ۲ - برای بالا بردن ضریب امنیتی کامپیوتر چه مواردی را در نرم افزار McAfee باید انجام دهیم؟
- ۳ - دیوار آتش چیست؟ توضیح دهید.
- ۴ - منظور از قرنطینه کردن فایل ها چیست؟
- ۵ - علت نیاز نرم افزارهای ضدویروس به بروزرسانی چیست؟



۱ - سیستم امنیتی را که جهت محافظت از شبکه داخلی در مقابل نفوذ افراد از خارج شبکه طراحی شده است ، را می گویند.

الف) Firewall ب) Proxy Server
ج) Router د) Security System

۲ - کدام سربرگ نرم افزار McAfee وظیفه مقابله با نامه های مزاحم و ناخواسته را دارد؟

الف) SpamKiller ب) Privacy Service
ج) Personal Firewall+ د) VirusScan

۳ - کدام سربرگ نرم افزار McAfee وظیفه ویروسیابی کامپیوتر را دارد؟

الف) My Security Center ب) SpamKiller
ج) Personal Firewall+ د) VirusScan

۴ - توسط کدام سربرگ نرم افزار McAfee می توان ضریب وضعیت امنیتی کامپیوتر را مشاهده نمود؟

الف) My Security Center ب) Personal Firewall+
ج) Privacy Service د) SpamKiller

۵ - برای بروزرسانی نرم افزار McAfee از دکمه استفاده می شود.

الف) Support ب) Online ج) Update د) Register



دستور کار آزمایشگاه



- ۱ - نرم افزار **McAfee** را بر روی کامپیوتر خود نصب نمایید.
- ۲ - یک دیسکت را در درایو قرار داده و به کمک نرم افزار **McAfee** ویروس یابی نمایید.
- ۳ - یک **CD** را در درایو قرار داده و به کمک نرم افزار **McAfee** ویروس یابی نمایید. توضیح دهید که اگر بر روی **CD** ویروس قرار داشته باشد چه اتفاقی می افتد. آیا می توان ویروس را حذف نمود؟
- ۴ - وضعیت امنیت کامپیوتر خود را بررسی کرده و یادداشت نمایید.
- ۵ - به کمک نرم افزار **McAfee** یک دیسک نجات برای کامپیوتر خود بسازید.
- ۶ - از طریق اینترنت نرم افزار **McAfee** را بروزرسانی نمایید.



فصل	سؤال	الف	ب	ج	د
چهارم	۱	✓			
	۲	✓			
	۳				✓
	۴	✓			
	۵			✓	

توانایی ششم

کار با نرم افزار ضد ویروس Norton

هدفهای رفتاری :

پس از مطالعه این توانایی از فراگیر انتظار می رود که :

- ☒ نرم افزار Norton Antivirus را نصب نماید.
- ☒ قسمت های مختلف نرم افزار Norton Antivirus را نام برده و کاربرد هر یک را توضیح دهد.
- ☒ عملیات ویروسیابی را به کمک نرم افزار Norton Antivirus انجام دهد.
- ☒ نرم افزار Norton Antivirus را از طریق اینترنت بروزرسانی نماید.

زمان نظری : ----

زمان عملی : ۴ ساعت



۶-۱ آشنایی با نرم افزار Norton Antivirus

این نرم افزار توسط شرکت Symantec طراحی شده است و در حدود ۲۸٪ بازار نرم افزارهای ضد ویروس در اختیار این نرم افزار است و بیش از ۳۵ میلیون کاربر در سطح دنیا دارد. از مهمترین مزایای این ضد ویروس، به روزرسانی ساده و سریع آن توسط سایت <http://www.symantec.com> است. در این کتاب، از نسخه ۲۰۰۴ نرم افزار Norton Antivirus استفاده شده است.

۶-۲ نصب نرم افزار Norton Antivirus

جهت نصب نرم افزار Norton Antivirus عملیات زیر را انجام می دهیم :



NAVSETUP.EXE
Norton AntiVirus NAVSetup
Symantec Corporation

✓ **CD** نصب نرم افزار Norton Antivirus را در درایو قرار داده و

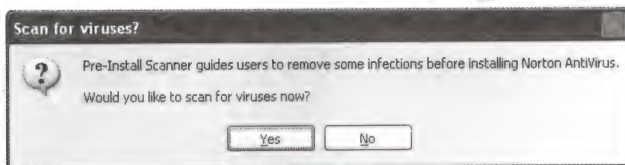
فایل NAVSetup.exe را اجرا می کنیم.

شکل (۶-۱) آیکن برنامه نصب Norton Antivirus

✓ پنجره ای مطابق شکل زیر ظاهر می شود. در این پنجره سؤال می شود که آیا می خواهید برنامه

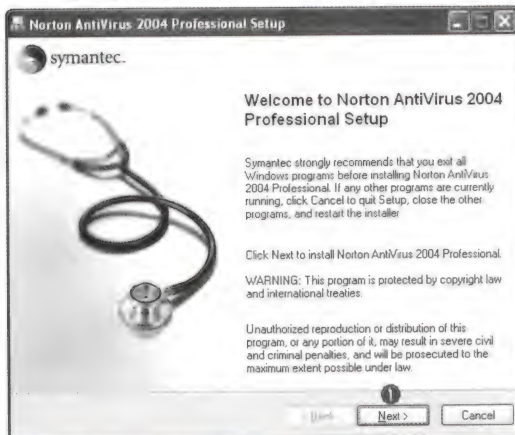
نصب، قبل از نصب ضد ویروس Norton، کامپیوتر شما را ویروس یابی کند. در صورت تمایل

دکمه را کلیک می کنیم.



شکل (۶-۲) پنجره محاوره ای سؤال در مورد ویروس یابی

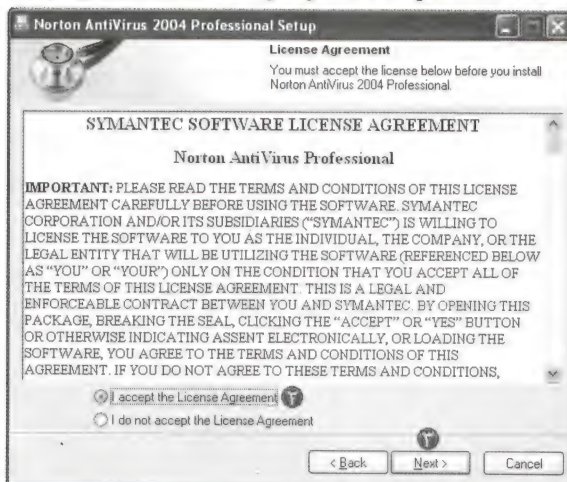
✓ پنجره خوش آمد گویی نصب ظاهر می شود. دکمه را جهت ادامه نصب کلیک می کنیم.



شکل (۶-۳) پنجره خوش آمدگویی نصب Norton Antivirus 2004

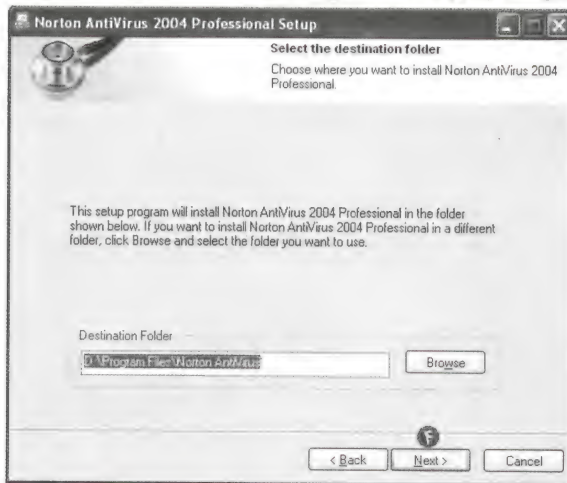


✓ در پنجره بعد، موافقتنامه مجوز استفاده از نرم‌افزار نمایش داده می‌شود. برای قبول این موافقتنامه، گزینه ☐ I accept the License Agreement را انتخاب کرده و دکمه را کلیک کنید.



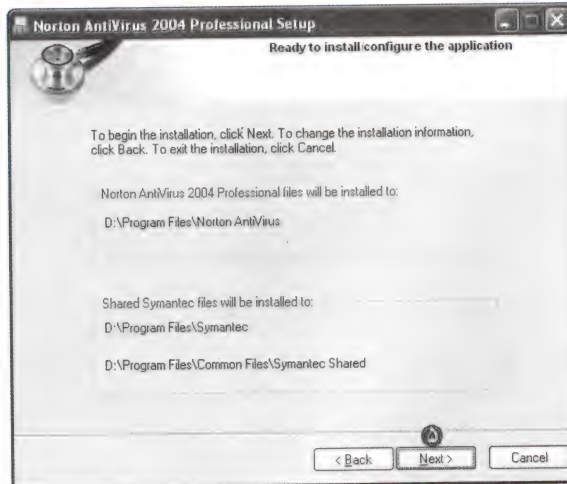
شکل (۴-۶) پنجره موافقتنامه مجوز استفاده از نرم‌افزار Norton Antivirus 2004

✓ در پنجره بعدی محل نصب نرم‌افزار مشخص شده است. می‌توانیم به کمک دکمه محل نصب برنامه را تغییر دهیم، جهت ادامه کار دکمه را کلیک می‌کنیم.



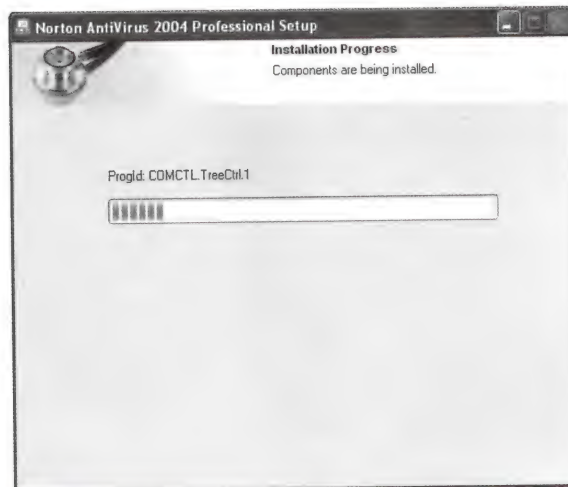
شکل (۵-۶) پنجره تعیین محل نصب نرم‌افزار

✓ در پنجره بعد، محل نصب نرم‌افزار و محل کپی کردن فایل‌های مورد نیاز آن نمایش داده می‌شود. اگر می‌خواهید این محل‌ها را تغییر دهید، دکمه را کلیک کنید. برای ادامه نصب دکمه را کلیک نمایید.



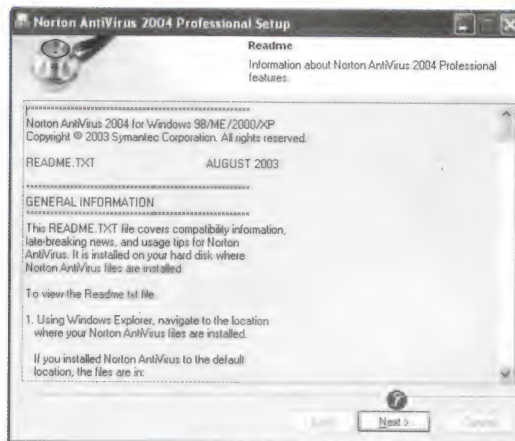
شکل (۶-۶) پنجره نمایش محل نصب نرم افزار

✓ پنجره کپی کردن فایل های نرم افزار Norton Antivirus ظاهر می شود و عملیات کپی فایل ها انجام می شود.



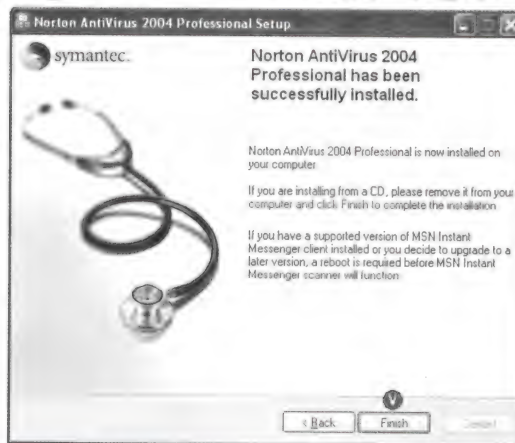
شکل (۶-۷) پنجره کپی فایل ها و عملیات نصب نرم افزار Norton Antivirus

✓ بعد از انجام عملیات نصب، پنجره **Readme** ظاهر می شود. در این پنجره توضیحاتی در مورد امکانات و نحوه استفاده از نرم افزار Norton Antivirus نمایش داده شده است. برای ادامه کار دکمه **Next >** را کلیک می کنیم.



شکل (۸-۶) پنجره Readme

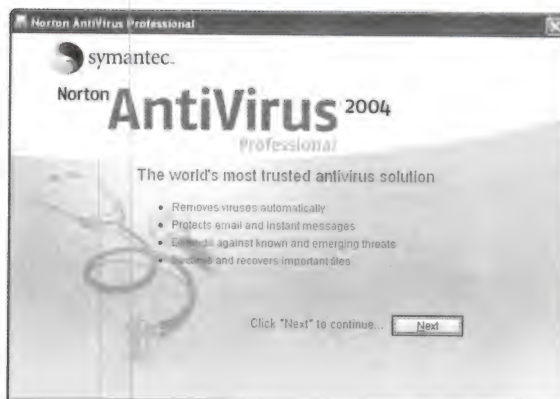
✓ پنجره پایانی نصب ظاهر می‌شود. بر روی دکمه **Finish** کلیک می‌کنیم.



شکل (۹-۶) پنجره پایانی نصب نرم‌افزار Norton Antivirus

✓ پس از اتمام عملیات نصب ،

پنجره‌ای مطابق شکل زیر ظاهر می‌شود. در این پنجره دکمه **Next >** را کلیک می‌کنیم.

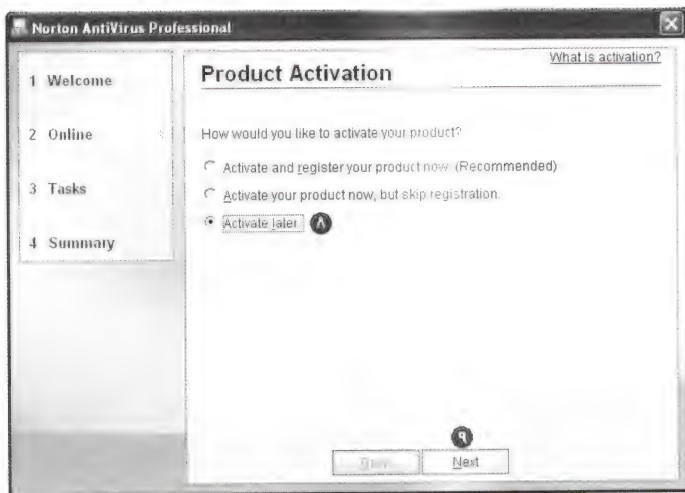


شکل (۱۰-۶) پنجره معرفی نرم‌افزار

Norton Antivirus

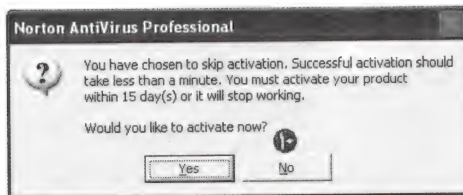


✓ در پنجره بعد از ما خواسته می شود که نرم افزار خود را فعال کنیم. در صورتیکه نرم افزار نصب شده
کیبی غیر مجاز نباشد و به اینترنت نیز متصل باشیم، گزینه اول را انتخاب کرده و دکمه **Next**
را کلیک می کنیم تا نرم افزار **Norton Antivirus** خود را فعال کنیم. در غیر این صورت گزینه سوم
(**Activate later**) فعال سازی در آینده را انتخاب کرده و دکمه **Next** را کلیک می کنیم.



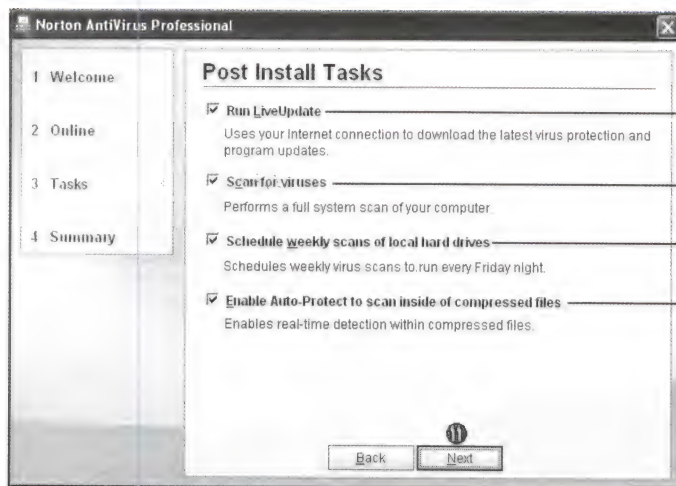
شکل (۶-۱۱) پنجره فعال سازی نرم افزار Norton Antivirus

✓ در صورتیکه در پنجره قبل گزینه سوم را انتخاب کرده باشیم، پنجره ای ظاهر می شود با این پیغام
که شما باید نرم افزار خود را ظرف مدت ۱۵ روز فعال نمایید. آیا می خواهید حالا نرم افزار خود را
فعال کنید؟ دکمه **No** را کلیک می کنیم.



شکل (۶-۱۲) پنجره سؤال در مورد فعال سازی

✓ در پنجره بعدی کارهایی که نرم افزار **Norton Antivirus** باید انجام دهد مشخص می شود. موارد
مورد نظر را انتخاب کرده و دکمه **Next** را کلیک می کنیم.



اجرای برنامه Live Update جهت دریافت آخرین اطلاعات محافظت در مقابل ویروسها و دریافت آخرین تغییرات نرم افزار

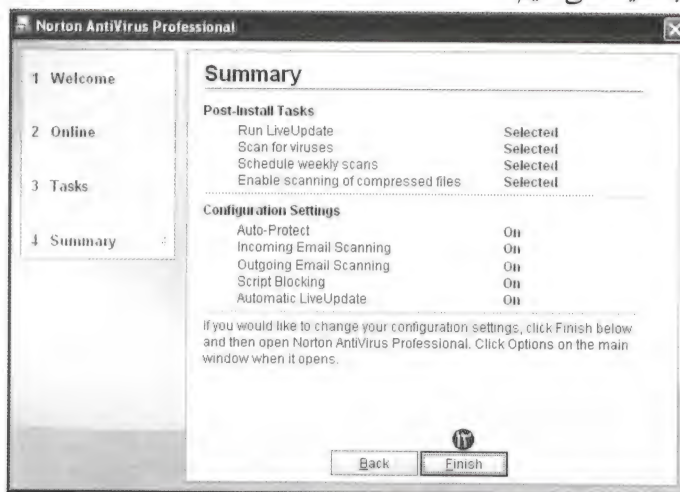
ویروس یابی کامل کامپیوتر شما

زمانبندی اجرای ویروس یابی هفتگی دیسکهای سخت

فعال کردن ویروس یابی داخل فایل های فشرده

شکل (۶-۱۳) پنجره تعیین کارهایی که نرم افزار Norton Antivirus باید انجام دهد

✓ در پایان خلاصه ای از کارهای انجام شده نمایش داده می شود. دکمه Finish را جهت اتمام عملیات نصب کلیک می کنیم.




شکل (۶-۱۴) خلاصه ای از عملیات و تنظیمات انجام شده



۳-۶ شناسایی و پاکسازی ویروسها با نرم افزار Norton Antivirus

همانند نرم افزار McAfee نرم افزار Norton Antivirus نیز پس از نصب، بصورت مقیم در حافظه قرار می گیرد. در ضمن هر بار که کامپیوتر را روشن کنیم این نرم افزار به صورت خودکار اجرا شده و در حافظه قرار می گیرد. هر فایل یا پوشه ای را که باز کنیم، نرم افزار Norton بصورت خودکار فایل های داخل آن را پوشه را بررسی می کند و در صورتیکه فایل ویروسی پیدا کند بلافاصله پیغامی را نمایش می دهد و از فعالیت ویروس جلوگیری می کند.

گاهی اوقات ممکن است بخواهیم تمام یا بخشی از فایل های کامپیوتر را ویروسیابی کنیم. برای ویروسیابی کامپیوتر عملیات زیر را انجام می دهیم:

✓ بر روی آیکن  در سینی نوار کار، دوبار کلیک می کنیم.

آیکن نرم افزار
ضد ویروس Norton



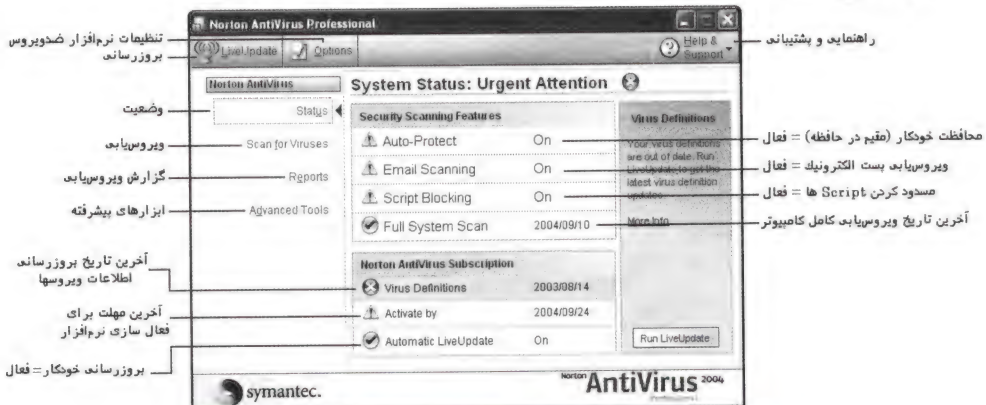
شکل (۱۵-۶) آیکن نرم افزار ضد ویروس Norton

✓ پنجره برنامه ضد ویروس Norton، ظاهر می شود. در این پنجره مشخصاتی از وضعیت فعلی و

Scan for Viruses

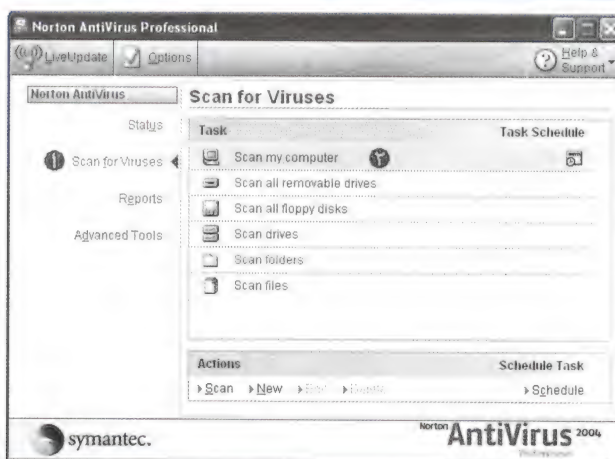
عملیات گذشته ضد ویروس نمایش داده می شود. جهت ویروسیابی بر روی دکمه

کلیک می کنیم.



شکل (۱۶-۶) پنجره اصلی نرم افزار Norton Antivirus - قسمت Status

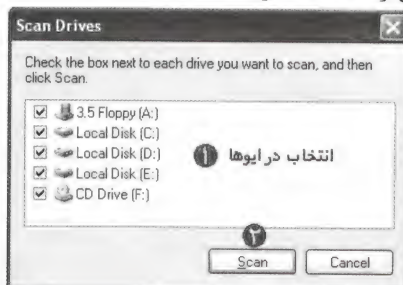
✓ پنجره ای مطابق شکل زیر ظاهر می شود.



شکل (۱۷-۶) نرم افزار Norton Antivirus قسمت Scan for Viruses

در این پنجره دکمه‌های زیر وجود دارد :

- Scan my computer
با دوبار کلیک بر روی این دکمه، کلیه فایل‌های موجود در کامپیوتر ویروس‌یابی می‌شود.
- Scan all removable drives
با دوبار کلیک بر روی این دکمه، کلیه درایوهای قابل جابجایی نظیر فلاپی دیسک، **Flash Disk**، **CD Drive** و ... ویروس‌یابی می‌شود.
- Scan all floppy disks
با دوبار کلیک بر روی این دکمه، تمامی درایوهای فلاپی موجود در کامپیوتر ویروس‌یابی می‌شود.
- Scan drives
با دوبار کلیک بر روی این دکمه، پنجره‌ای باز می‌شود که می‌توان درایو یا درایوهای مورد نظر جهت ویروس‌یابی را انتخاب نمود.



شکل (۱۸-۶) پنجره انتخاب درایوها جهت ویروس‌یابی

☐ Scan folders

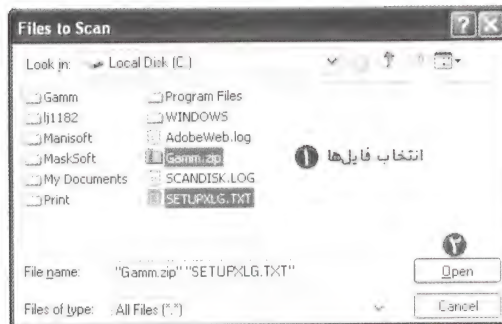
با دوبار کلیک بر روی این دکمه، پنجره‌ای باز می‌شود که می‌توان پوشه یا پوشه‌های مورد نظر جهت ویروسیابی را انتخاب نمود.



شکل (۶-۱۹) پنجره انتخاب پوشه‌ها جهت ویروسیابی

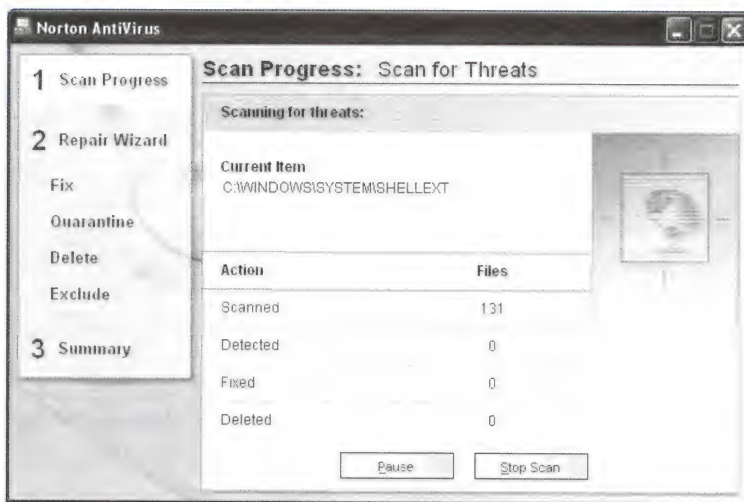
☐ Scan files

با دوبار کلیک بر روی این دکمه، پنجره‌ای باز می‌شود که می‌توان فایل یا فایل‌های مورد نظر جهت ویروسیابی را انتخاب نمود.



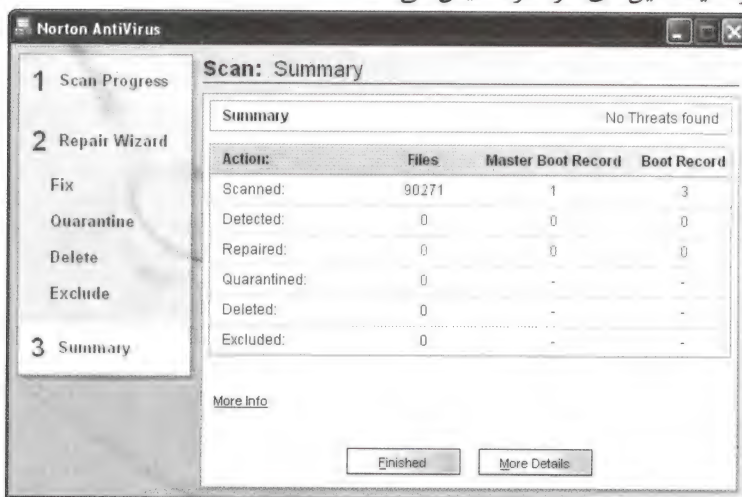
شکل (۶-۲۰) پنجره انتخاب فایل‌ها جهت ویروسیابی

☑ پس از انجام یکی از موارد فوق، پنجره‌ای مطابق شکل زیر باز می‌شود و فایل‌ها، پوشه‌ها یا درایوهایی که مشخص کرده‌ایم را ویروسیابی می‌کند.



شکل (۶-۲۱) پنجره ویروس‌یابی فایل‌ها و پوشه‌های تعیین شده

✓ در صورتیکه فایل ویروسی در کامپیوتر پیدا شود، نرم‌افزار *Antivirus* ویروس فایل آلوده را پاک می‌کند. در پایان گزارشی نمایش داده می‌شود که تعداد فایل‌های بررسی شده و تعداد فایل‌های آلوده و وضعیت فایل‌های آلوده را نمایش می‌دهد.





شکل (۶-۲۲) پنجره نمایش نتیجه عملیات ویروس‌یابی



۴-۶ بروزرسانی نرم افزار Norton Antivirus

همانطور که در فصل قبل نیز اشاره کردیم ، ممکن است ظرف یک هفته یا چند روز ویروسهای جدیدی توسط افراد خرابکار تولید شود. نرم افزارهای ضد ویروس فقط قادر به شناسایی ویروسهای شناخته شده هستند بنابراین نیاز است که هر چند روز یکبار آنها را بروزرسانی نماییم. شرکتهای تولید کننده نرم افزارهای ضد ویروس، آخرین ویروسهای را در سطح دنیا شناسایی می کنند و پس از تشخیص عملکرد و نحوه پاک کردن آنها، اطلاعات ویروس و نحوه حذف آن را در سایتهای اینترنتی خود قرار می دهند. در ضمن امکان بروزرسانی نرم افزارهای ضد ویروس را از طریق اینترنت به کاربران خود می دهند.

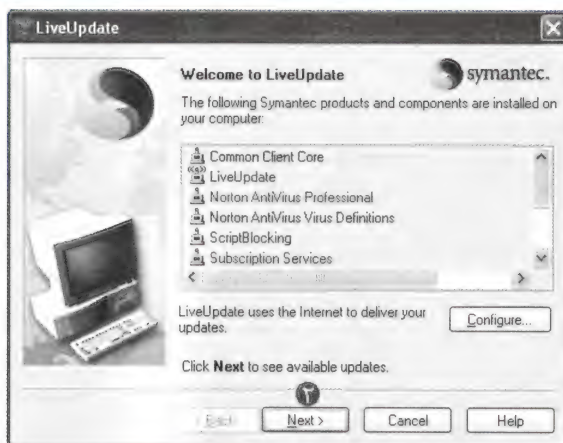
جهت بروزرسانی نرم افزار Norton Antivirus عملیات زیر را انجام می دهیم :

- ☒ ابتدا به اینترنت متصل می شویم.
- ☒ بر روی آیکن  در سینی نوار کار، دوبار کلیک می کنیم.
- ☒ در پنجره اصلی نرم افزار *Norton Antivirus* بر روی دکمه  کلیک می کنیم.



شکل (۲۳-۶) پنجره اصلی برنامه Norton Antivirus

- ☒ پنجره *Live Update* ظاهر می شود. در این پنجره دکمه  را کلیک می کنیم.



شکل (۶-۲۴) پنجره Live Update

- ☒ برنامه **Live Update** به اینترنت متصل شده و اطلاعات شناسایی و حذف ویروسهای جدید را دریافت می‌کند.



۱ - وظیفه برنامه Live Update در نرم افزار Norton Antivirus چیست؟

۲ - علت بروزرسانی نرم افزارهای ضد ویروس چیست؟



۱ - کدام نرم افزار ضد ویروس زیر توسط شرکت Symantec طراحی شده است؟

الف) Dr Web

ب) Norton Antivirus

ج) McAfee Virus Scan

د) Panda Antivirus

۲ - کدام نرم افزار زیر ضد ویروس محسوب نمی شود؟

الف) Norton Utility

ب) Norton Antivirus

ج) McAfee

د) Panda

۳ - برای بروزرسانی نرم افزار Norton Antivirus از کدام دکمه استفاده می شود؟

الف) Status

ب) Online

ج) Live Update

د) Register

۴ - در نرم افزار Norton Antivirus برای ویروس یابی یک فایل در درایو C بهتر است از کدام دکمه زیر استفاده شود؟

الف) Scan my computer

ب) Scan folders

ج) Scan drives

د) Scan files

۵ - در نرم افزار Norton Antivirus برای ویروس یابی فلاپی دیسک بهتر است از کدام دکمه زیر استفاده شود؟

الف) Scan my computer

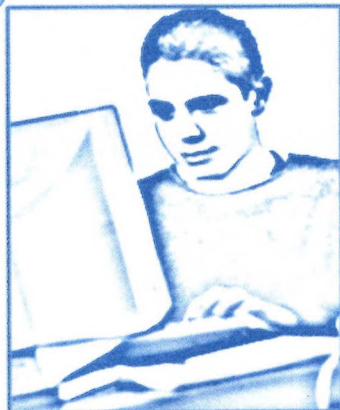
ب) Scan all floppy disks

ج) Scan folders

د) Scan files



دستور کار آزمایشگاه



- ۱ - نرم افزار Norton Antivirus را بر روی کامپیوتر خود نصب نمایید.
- ۲ - یک دیسکت را Write Protect کرده و در درایو قرار داده و به کمک نرم افزار Norton Antivirus ویروس یابی نمایید. در صورت یافتن ویروس چه اتفاقی می افتد؟
- ۳ - درایو C کامپیوتر را ویروس یابی نمایید.
- ۴ - فقط پوشه ویندوز را ویروس یابی نمایید.
- ۵ - فقط فایل Calc.exe در پوشه Windows\system32 را ویروس یابی نمایید.
- ۶ - از طریق اینترنت نرم افزار Norton Antivirus را بروزرسانی نمایید.



فصل	سؤال	الف	ب	ج	د
ششم	۱		✓		
	۲	✓			
	۳			✓	
	۴				✓
	۵		✓		